Instalar y configurar vSphere

Actualización 2
Modificada el 20 abril de 2022
VMware vSphere 6.5
VMware ESXi 6.5
vCenter Server 6.5

Puede encontrar la documentación técnica más actualizada en el sitio web de VMware:

https://docs.vmware.com/es/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Spain, S.L.
Calle Rafael Boti 26
2.ª planta
Madrid 28023
Tel.: +34 914125000
www.vmware.com/es

Contenido

Acerca de la instalación y configuración de vSphere

En la documentación de *instalación y configuración de vSphere* se describe cómo instalar y configurar VMware vCenter Server®, implementar VMware vCenter® Server Appliance™ e instalar y configurar VMware ESXi™.

Audiencia prevista

El tema sobre *instalación y configuración de vSphere* está pensado para administradores experimentados que desean instalar y configurar vCenter Server, implementar y configurar vCenter Server Appliance, e instalar y configurar ESXi.

Esta información está escrita para administradores del sistema de Windows y Linux expertos que están familiarizados con la tecnología de máquina virtual y las operaciones de centro de datos. La información sobre el uso de Image Builder y VMware vSphere® Auto Deploy™ está escrita para administradores que tienen experiencia con Microsoft PowerShell y VMware vSphere® PowerCLI™.

vSphere Web Client y vSphere Client

Las instrucciones para las tareas en esta guía se basan en vSphere Web Client. También puede realizar la mayoría de las tareas en esta guía con la nueva instancia de vSphere Client. La terminología, la topología y el flujo de trabajo de la interfaz de usuario de la nueva instancia de vSphere Client están estrechamente alineados con los mismos aspectos y elementos de la interfaz de usuario de vSphere Web Client. Puede aplicar las instrucciones de vSphere Web Client a la nueva instancia de vSphere Client, a menos que se indique lo contrario.

Nota No todas las funcionalidades de vSphere Web Client se implementaron para vSphere Client en la versión de vSphere 6.5. Para obtener una lista actualizada de las funcionalidades no compatibles, consulte la *Guía sobre actualizaciones de las funcionalidades en vSphere Client* en http://www.vmware.com/info?id=1413.

Glosario de publicaciones técnicas de VMware

Publicaciones técnicas de VMware proporciona un glosario de términos que podrían resultarle desconocidos. Para ver las definiciones de los términos que se utilizan en la documentación técnica de VMware, vaya a http://www.vmware.com/support/pubs.

Información actualizada

Esta guía *Instalación y configuración de vSphere* se actualiza con cada versión del producto o cuando sea necesario.

En esta tabla se muestra el historial de actualizaciones de la guía *Instalación y configuración de vSphere*.

Revisión	Descripción
14 de abril de 2021	VMware ha cambiado el nombre del portal My VMware por VMware Customer Connect. Hemos actualizado esta guía para reflejar este cambio de nombre.
02 de abril de 2021	■ Se actualizó la lista de versiones de exploradores compatibles para vSphere Web Client en Requisitos de software de vSphere Web Client. ■ Se eliminó Internet Explorer como explorador web compatible para su uso con vSphere Web Client.
11 de agosto de 2020	En VMware, valoramos la inclusión. Para fomentar este principio entre nuestros clientes, nuestros partners y nuestra comunidad interna, estamos reemplazando parte de la terminología en nuestro contenido. Actualizamos esta guía para eliminar el lenguaje no inclusivo.
28 de abril de 2020	Se incluyó el requisito previo que requiere que, al implementar una nueva instancia de vCenter Server como parte de una implementación de Enhanced Linked Mode, se debe crear una copia de seguridad basada en imágenes de los nodos de vCenter Server existentes en el entorno. Puede utilizar la copia de seguridad como precaución en caso de que se produzca un error durante el proceso de implementación. Consulte Requisitos previos para implementar vCenter Server Appliance o el dispositivo de Platform Services Controller.
28 de junio de 2019	Se actualizó la configuración máxima de la instancia de vCenter Server Appliance con nodos integrados de Platform Services Controller y la instancia de vCenter Server con instalaciones externas de Platform Services Controller a las que es posible unirse mediante vCenter Enhanced Linked Mode en vCenter Enhanced Linked Mode.
26 FEB DE 2019	Se corrigió la descripción "Utilizado para la comunicación de nodo a nodo" para el puerto TCP 7444 en Puertos necesarios para vCenter Server y Platform Services Controller.
11 de septiembre de 2018	Correcciones menores.
10 DE JULIO DE 2018	Se actualizó Capítulo 3 Implementar vCenter Server Appliance y el dispositivo de Platform Services Controller para aclarar la compatibilidad con IPv4 e IPv6.

Revisión	Descripción
22 de junio de 2018	■ Se agrega una nota en Comandos de scripts de instalación y actualización que indica que el script `%firstboot` no se ejecuta si el arranque seguro está habilitado en el host ESXi. ■ Se agregan los puertos de VMware vSphere Authentication Proxy (7475 y 7476) a Puertos necesarios para vCenter Server y Platform Services Controller. ■ Se clarifica la lista de las copias de seguridad y recuperaciones no admitidas en Capítulo 7 Restaurar y crear copias de seguridad con base en imágenes de un entorno de vCenter Server; no son compatibles con vSphere Data Protection. ■ Se actualiza la información sobre vCenter High Availability para vCenter Embedded Linked Mode en vCenter Embedded Linked Mode para vCenter Server Appliance con instancia integrada de Platform Services Controller.
10 de mayo de 2018	■ Se agrega una nota que indica que **`Primer sitio predeterminado`** debe utilizarse como el nombre del sitio para la primera instancia al configurar una instancia de Embedded Linked Mode en Etapa 2 - Configure la instancia de vCenter Server Appliance recién implementada con Platform Services Controller integrado y Parámetros de configuración de implementación. ■ Se actualizan las descripciones de las plantillas `embedded_vCSA_replication_on_ESXi.json` y `embedded_vCSA_replication_on_VC.json` en Plantillas JSON para la implementación de CLI de vCenter Server Appliance y del dispositivo de Platform Services Controller.
7 de mayo de 2018	■ Se actualiza la descripción de vCenter Server con una instancia integrada de Platform Services Controller en Tipos de implementación de vCenter Server y Platform Services Controller para incluir la funcionalidad Enhanced Linked Mode. ■ Se agrega una notificación de que Embedded Linked Mode se admite a partir de vSphere 6.5 Update 2 en vCenter Embedded Linked Mode para vCenter Server Appliance con instancia integrada de Platform Services Controller. ■ Se cambia a 15 el número de instancias de vCenter Server Appliance que pueden vincularse en vCenter Embedded Linked Mode para vCenter Server Appliance con instancia integrada de Platform Services Controller. ■ Se agrega información sobre Embedded Linked Mode con replicación de solo lectura en vCenter Embedded Linked Mode para vCenter Server Appliance con instancia integrada de Platform Services Controller. ■ Se actualizan las instrucciones de Unirse a un dominio de vCenter Embedded Linked Mode. ■ Se actualiza la nota sobre los puertos 80 y 443 en Puertos necesarios para vCenter Server y Platform Services Controller. ■ Se agregan el parámetro de configuración `ports` y su descripción a la subsección de redes en Parámetros de configuración de implementación.
3 de mayo de 2018	Versión inicial.

Introducción a la instalación y configuración de vSphere

1

vSphere 6.5 proporciona diferentes opciones para la instalación y configuración. Para garantizar una implementación correcta de vSphere, comprenda las opciones de instalación y configuración, y la secuencia de tareas.

Los dos componentes principales de vSphere son ESXi y vCenter Server. ESXi es la plataforma de virtualización en la que puede crear y ejecutar máquinas virtuales y aplicaciones virtuales. vCenter Server es un servicio que funciona como un administrador central para los hosts de ESXi conectados en una red. vCenter Server permite agrupar y administrar los recursos de varios hosts.

Puede instalar vCenter Server en una máquina virtual o servidor físico con Windows, o implementar vCenter Server Appliance. vCenter Server Appliance es una máquina virtual preconfigurada y basada en Linux optimizada para la ejecución de vCenter Server y los componentes de vCenter Server. Es posible implementar vCenter Server Appliance en hosts ESXi 5.5 o posteriores, o bien en instancias de vCenter Server 5.5 o posteriores.

A partir de vSphere 6.0, todos los servicios de requisito previo para la ejecución de vCenter Server y los componentes de vCenter Server están integrados en VMware Platform Services Controller™. Puede implementar vCenter Server con un Platform Services Controller externo o integrado, pero deberá siempre instalar o implementar el Platform Services Controller antes de instalar o implementar vCenter Server.

Este capítulo incluye los siguientes temas:

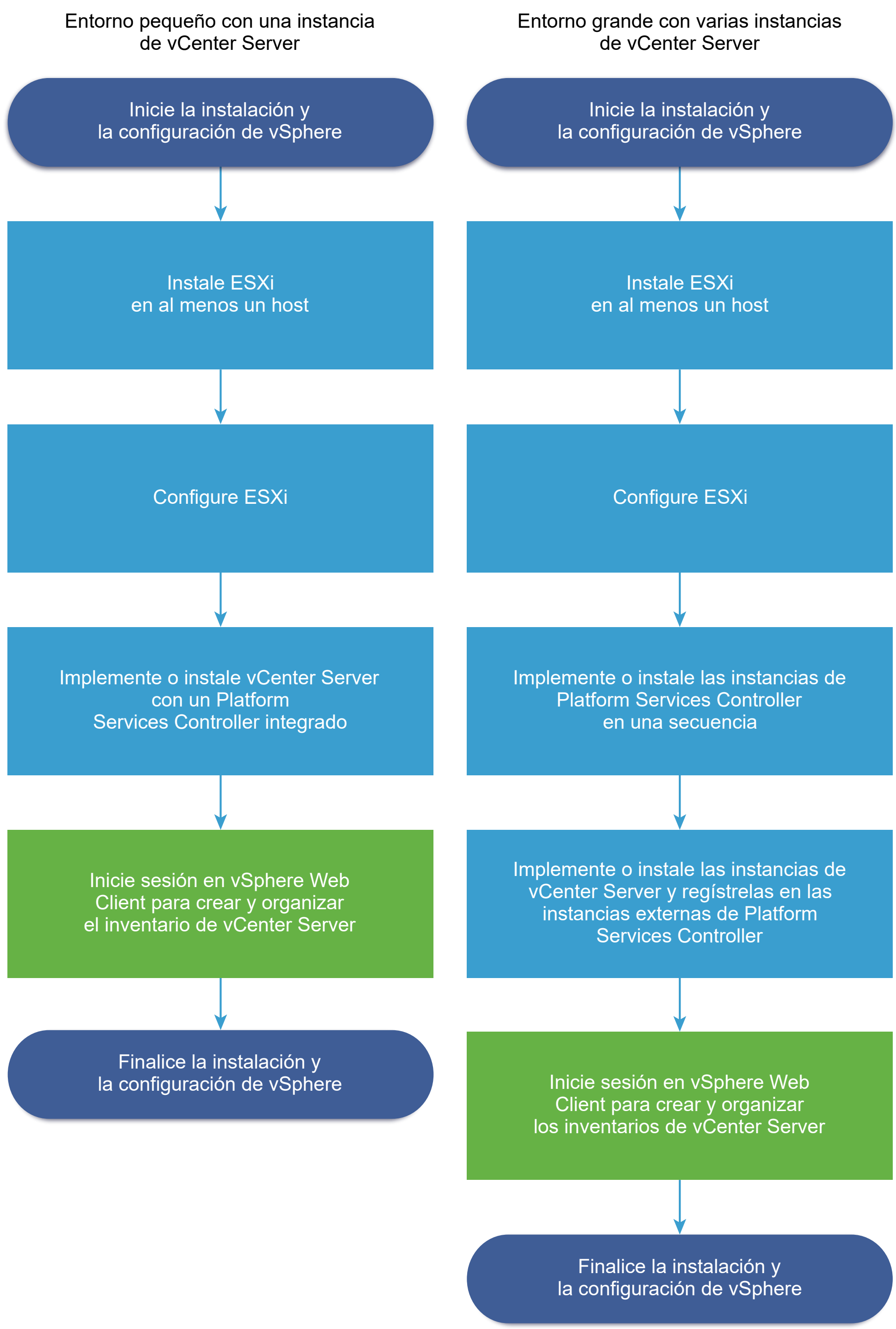
- Información general del proceso de instalación y configuración de vSphere
- Componentes y servicios de vCenter Server
- Descripción general de vCenter Server Appliance
- Tipos de implementación de vCenter Server y Platform Services Controller
- Comprender los sitios, nombres de dominio y dominios de vSphere
- Topologías de implementación con instancias de Platform Services Controller externas y alta disponibilidad
- vCenter Enhanced Linked Mode
- Acerca de los modos de evaluación y con licencia de ESXi

Información general del proceso de instalación y configuración de vSphere

vSphere es un producto sofisticado con varios componentes que puede instalar y configurar. A fin de garantizar una implementación correcta de vSphere, comprenda la secuencia de las tareas requeridas.

La instalación de vSphere incluye las siguientes tareas:

Figura 1-1. Flujo de trabajo de instalación y configuración de vSphere



1 Lea las notas de la versión de vSphere.

2 Instale ESXi.

   a Compruebe que el sistema cumpla con los requisitos de hardware mínimos. Consulte Requisitos de ESXi.

b Determine la opción de instalación de ESXi que desea utilizar. Consulte Opciones para instalar ESXi .

c Determine dónde desea ubicar y arrancar el instalador de ESXi. Consulte Opciones de medios para arrancar el instalador de ESXi. Si va a utilizar PXE para arrancar el instalador, compruebe que la infraestructura PXE de la red esté configurada correctamente. Consulte Arranque PXE del instalador de ESXi.

d Cree una hoja de cálculo con la información que necesitará al instalar ESXi. Consulte Información obligatoria para instalar ESXi.

e Instale ESXi.

- Instalar ESXi de forma interactiva
- Instalar o actualizar hosts mediante un script

Nota También puede aprovisionar hosts ESXi con vSphere Auto Deploy, pero vSphere Auto Deploy se instala junto con vCenter Server. Para aprovisionar hosts ESXi con Auto Deploy, debe implementar la instancia de vCenter Server Appliance o instalar vCenter Server.

3 Ajuste la configuración de red y arranque de ESXi, la consola directa y otras opciones. Consulte Configurar ESXi y Después de instalar y configurar ESXi.

4 Considere la posibilidad de configurar un servidor de Syslog para inicio de sesión remoto, a fin de garantizar que haya almacenamiento de disco suficiente para los archivos de registro. La configuración del registro en un host remoto es especialmente importante para hosts con almacenamiento local limitado. Consulte Espacio libre necesario para registro del sistema y Configurar Syslog en hosts ESXi.

5 Determine el modelo de implementación de vCenter Server y Platform Services Controller que sea apto para el entorno.

Consulte Tipos de implementación de vCenter Server y Platform Services Controller.

6 Implemente o instale vCenter Server y Platform Services Controller.

Puede implementar el dispositivo de vCenter Server Appliance o Platform Services Controller en un host ESXi o en una instancia de vCenter Server, o bien puede instalar vCenter Server y Platform Services Controller en una máquina virtual o en un servidor físico Windows.

Para implementar o instalar varias instancias de vCenter Server conectadas mediante una configuración Enhanced Linked Mode, regístrelas en instancias unidas de Platform Services Controller comunes o diferentes.

- Implemente el dispositivo de vCenter Server Appliance o Platform Services Controller.

  1 Consulte los temas en Requisitos de sistema para el dispositivo vCenter Server Appliance y Platform Services Controller y compruebe que el sistema cumpla con los requisitos de hardware y software para la implementación del dispositivo.

  2 Determine el método de implementación que desea utilizar.

Puede utilizar el método de GUI para implementar de manera interactiva el dispositivo. Puede utilizar el método de CLI para realizar una implementación silenciosa del dispositivo. Consulte Implementación de la GUI de vCenter Server Appliance y del dispositivo de Platform Services Controller y Implementación de CLI en vCenter Server Appliance y en el dispositivo de Platform Services Controller.

3 Utilice el tema Información requerida para implementar una instancia de vCenter Server Appliance o un dispositivo de Platform Services Controller para crear una hoja de trabajo con la información necesaria para la implementación de GUI, o utilice el tema Preparar el archivo de configuración JSON para la implementación de CLI a fin de crear las plantillas JSON para la implementación de CLI.

4 Implemente el dispositivo.

- Instale vCenter Server o Platform Services Controller en una máquina virtual o un servidor físico Windows.

  1 Compruebe que su sistema cumpla con los requisitos de hardware y software para la instalación de vCenter Server. Consulte Requisitos de vCenter Server para Windows.

  2 (Opcional) Configure una base de datos de vCenter Server externa. Consulte Preparar las bases de datos de vCenter Server para la instalación.

  Para un entorno con hasta 20 hosts y 200 máquinas virtuales, puede utilizar la base de datos PostgreSQL integrada. Para entornos de producción y gran escala, configure una base de datos externa, debido a que la migración desde la base de datos PostgreSQL integrada a una base de datos externa no es un proceso manual sencillo.

  3 Cree una hoja de cálculo con la información que necesita para la instalación. Consulte Información necesaria para instalar vCenter Server o Platform Services Controller en Windows.

  4 Instale vCenter Server con una instancia de Platform Services Controller integrada Platform Services Controller, o vCenter Server con una instancia de Platform Services Controller externa.

7 Conéctese a vCenter Server desde vSphere Web Client. Consulte Capítulo 5 Después de instalar vCenter Server o implementar vCenter Server Appliance.

8 Configure la instancia de vCenter Server Appliance o vCenter Server. Consulte *Configuración de vCenter Server Appliance* y *Administrar vCenter Server y hosts*.

Componentes y servicios de vCenter Server

vCenter Server proporciona una plataforma centralizada para la administración, el funcionamiento, el aprovisionamiento de recursos y la evaluación del rendimiento de las máquinas virtuales y los hosts.

Cuando instale vCenter Server con una instancia de Platform Services Controller integrada o implemente vCenter Server Appliance con una instancia de Platform Services Controller integrada, vCenter Server, los componentes de vCenter Server y los servicios incluidos en Platform Services Controller se implementan en el mismo sistema.

Cuando instale vCenter Server con una instancia de Platform Services Controller externa o implemente vCenter Server Appliance con una instancia de Platform Services Controller externa, vCenter Server y los componentes de vCenter Server se implementan en un sistema y los servicios incluidos en Platform Services Controller se implementan en otro sistema.

Los siguientes componentes se incluyen en las instalaciones de vCenter Server y vCenter Server Appliance:

- El grupo de servicios de infraestructura de VMware Platform Services Controller contiene vCenter Single Sign-On, el servicio de licencias, Lookup Service y VMware Certificate Authority.
- El grupo de servicios de vCenter Server contiene vCenter Server, vSphere Web Client, vSphere Auto Deploy y vSphere ESXi Dump Collector. vCenter Server para Windows también contiene VMware vSphere Syslog Collector. vCenter Server Appliance también contiene el servicio de la extensión de VMware vSphere Update Manager.

Nota A partir de vSphere 6.5, todos los servicios de vCenter Server y algunos de los servicios de Platform Services Controller se ejecutan como procesos secundarios del servicio VMware Service Lifecycle Manager.

Servicios instalados con VMware Platform Services Controller

vCenter Single Sign-On

El servicio de autenticación de vCenter Single Sign-On proporciona servicios de autenticación segura a los componentes de software de vSphere. Al utilizar vCenter Single Sign-On, los componentes de vSphere se comunican entre sí a través de un mecanismo de intercambio seguro de tokens, en lugar de requerir que cada componente autentique a un usuario por separado con un servicio de directorio como Active Directory. vCenter Single Sign-On implementa un dominio de seguridad interno (por ejemplo, vsphere.local), donde las soluciones y los componentes de vSphere se registran durante el proceso de instalación o actualización, lo que proporciona un recurso de infraestructura. vCenter Single Sign-On puede realizar la autenticación de los usuarios desde sus propios usuarios y grupos internos o puede conectarse a servicios de directorio externos de confianza, como Microsoft Active Directory. A continuación, los usuarios autenticados pueden recibir asignaciones de permisos o roles registrados y basados en soluciones dentro de un entorno de vSphere.

Se requiere vCenter Single Sign-On con vCenter Server.

Servicio de licencias de vSphere

El servicio de licencias de vSphere proporciona funcionalidades comunes de administración e inventario de licencias a todos sistemas vCenter Server que estén conectados a Platform Services Controller o varias instancias de Platform Services Controller asociadas.

VMware Certificate Authority

VMware Certificate Authority (VMCA) aprovisiona cada host ESXi con un certificado firmado que tiene VMCA como la entidad de certificación raíz de forma predeterminada. El aprovisionamiento ocurre cuando el host ESXi se agrega a vCenter Server de forma explícita o como parte del proceso de instalación del host ESXi. Todos los certificados de ESXi se almacenan localmente en el host.

Para obtener información sobre todos los servicios y las capacidades de Platform Services Controller, consulte *Administrar Platform Services Controller*.

Servicios instalados con vCenter Server

Estos componentes adicionales se instalan de forma silenciosa cuando se instala vCenter Server. Los componentes no pueden instalarse por separado, puesto que no poseen sus propios instaladores.

PostgreSQL

Una versión integrada de la distribución de VMware de la base de datos de PostgreSQL para vSphere y vCloud Hybrid Services.

vSphere Web Client

vSphere Web Client permite conectarse a instancias de vCenter Server mediante un explorador web y, de esta forma, podrá administrar su infraestructura vSphere.

vSphere Client

La nueva interfaz de usuario que permite conectarse a instancias de vCenter Server por medio de un explorador web. La terminología, la topología y el flujo de trabajo están estrechamente alineados con los mismos aspectos y elementos de la interfaz de usuario de vSphere Web Client.

Nota No todas las funcionalidades de vSphere Web Client se implementaron para vSphere Client en la versión de vSphere 6.5. Para obtener una lista actualizada de las funcionalidades no compatibles, consulte la *Guía sobre actualizaciones de las funcionalidades en vSphere Client* en http://www.vmware.com/info?id=1413.

vSphere ESXi Dump Collector

Herramienta de soporte de vCenter Server. Puede configurar ESXi para guardar la memoria VMkernel en un servidor de red, en lugar de un disco, cuando el sistema detecta un error crítico. vSphere ESXi Dump Collector recopila los volcados de memoria en la red.

VMware vSphere Syslog Collector

La herramienta de soporte de vCenter Server en Windows que permite la generación de registros de la red y la combinación de registros de varios hosts. Puede utilizar vSphere Syslog Collector para dirigir los registros del sistema ESXi a un servidor de la red, en lugar de a un disco local. La cantidad máxima recomendada de hosts admitidos para la recopilación de registros es 30. Para obtener información sobre la configuración de vSphere Syslog Collector, consulte http://kb.vmware.com/kb/2021652.

vCenter Server Appliance utiliza el servicio integrado Rsyslog del sistema operativo Linux. Para obtener información acerca de cómo redirigir los archivos de registro a otro equipo con la interfaz de administración del dispositivo, consulte *Configurar vCenter Server Appliance*.

vSphere Auto Deploy

La herramienta de soporte de vCenter Server que puede aprovisionar cientos de hosts físicos con software ESXi. Se puede especificar la imagen que se implementará y los hosts que se aprovisionarán con esa imagen. O bien, puede especificar perfiles de host para aplicar a los hosts y una ubicación de vCenter Server (carpeta o clúster) para cada host.

Extensión de VMware vSphere Update Manager

Update Manager permite la administración centralizada y automatizada de revisiones y versiones para VMware vSphere y ofrece soporte para hosts ESXi, máquinas virtuales y dispositivos virtuales VMware. La extensión de VMware vSphere Update Manager es un servicio opcional únicamente de vCenter Server Appliance6.5.

Descripción general de vCenter Server Appliance

vCenter Server Appliance es una máquina virtual preconfigurada basada en Linux que está optimizada para ejecutar vCenter Server y los servicios asociados.

vCenter Server Appliance reduce el tiempo de implementación de vCenter Server y los servicios asociados, y ofrece una alternativa de bajo costo a la instalación de vCenter Server basada en Windows.

El paquete de vCenter Server Appliance contiene los siguientes componentes de software:

- Project Photon OS® 1.0
- El grupo de servicios de infraestructura de Platform Services Controller
- El grupo de servicios de vCenter Server
- PostgreSQL
- Extensión de VMware vSphere Update Manager

La versión 6.5 de vCenter Server Appliance se implementa con la versión 10 del hardware virtual, que admite 64 CPU virtuales por máquina virtual en ESXi.

vCenter Server Appliance utiliza la base de datos de PostgreSQL integrada, que posee escalabilidad de hasta 2.000 hosts y 35.000 máquinas virtuales. Durante la implementación, puede seleccionar el tamaño de vCenter Server Appliance para el tamaño del entorno de vSphere y el tamaño de almacenamiento para los requisitos de base de datos.

A partir de vSphere 6.5, vCenter Server utiliza el servicio de extensión de VMware vSphere Update Manager. Ya no se requiere una instancia externa de VMware Update Manager para la administración automatizada y centralizada de revisiones y versiones de vSphere. Para obtener más información sobre los servicios de vCenter Server y Platform Services Controller, consulte Componentes y servicios de vCenter Server.

A partir de vSphere 6.5, vCenter Server Appliance admite alta disponibilidad. Para obtener más información sobre la configuración de vCenter Server Appliance en un clúster de vCenter de alta disponibilidad, consulte *Disponibilidad de vSphere*.

A partir de vSphere 6.5, vCenter Server Appliance y el dispositivo de Platform Services Controller admiten copia de seguridad y restauración basada en archivos. Para obtener información sobre las operaciones de copia de seguridad y restauración, consulte Capítulo 6 Restaurar vCenter Server Appliance y crear una copia de seguridad de ella con base en archivos.

Para obtener información sobre los máximos de vCenter Server Appliance, consulte la documentación de *Máximos de configuración*.

Tipos de implementación de vCenter Server y Platform Services Controller

Puede implementar vCenter Server Appliance o instalar vCenter Server para Windows con una instancia de Platform Services Controller integrada o externa. También puede implementar Platform Services Controller como dispositivo o instalarlo en Windows. Si es necesario, puede usar un entorno de sistema operativo mixto.

Antes de implementar vCenter Server Appliance o instalar vCenter Server para Windows, debe determinar el modelo de implementación que sea adecuado para su entorno. Para cada implementación o instalación, debe seleccionar uno de los tres tipos de implementación.

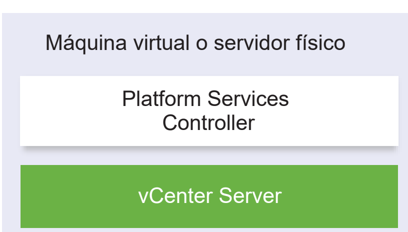
Tabla 1-1. Tipos de implementación de vCenter Server y Platform Services Controller

Tipo de implementación	Descripción
vCenter Server con una instancia de Platform Services Controller integrada	Todos los servicios que se incluyen en el paquete con Platform Services Controller se implementan junto con los servicios de vCenter Server en la misma máquina virtual o el mismo servidor físico.
Platform Services Controller	Solo los servicios que se incluyen en el paquete con Platform Services Controller se implementan en la máquina virtual o el servidor físico.
vCenter Server con una instancia de Platform Services Controller externa (Requiere una instancia de Platform Services Controller externa)	Solo los servicios de vCenter Server se implementan en la máquina virtual o el servidor físico. Debe registrar dicha instancia de vCenter Server con una instancia de Platform Services Controller que haya implementado o instalado anteriormente.

vCenter Server con una instancia de Platform Services Controller integrada

El uso de una instancia integrada de Platform Services Controller da como resultado una implementación independiente que tiene su propio dominio de vCenter Single Sign-On con un único sitio. A partir de vSphere 6.5 Update 2, otras instancias de vCenter Server con una instancia de Platform Services Controller integrada pueden combinarse para habilitar Enhanced Linked Mode.

Figura 1-2. vCenter Server con una instancia de Platform Services Controller integrada



La instalación de vCenter Server con una instancia integrada de Platform Services Controller posee las siguientes ventajas:

- La conexión entre vCenter Server y Platform Services Controller no se realiza a través de la red, y vCenter Server no está propenso a interrupciones causadas por problemas de conectividad y resolución de nombres entre vCenter Server y Platform Services Controller.
- Si instala vCenter Server en máquinas virtuales o servidores físicos con Windows, necesita menos licencias de Windows.
- Debe administrar menos máquinas virtuales o servidores físicos.

Puede configurar vCenter Server Appliance con una instancia de Platform Services Controller integrada en la configuración de alta disponibilidad de vCenter. Para obtener información, consulte *Disponibilidad de vSphere*.

Nota Después de implementar o instalar vCenter Server con una instancia de Platform Services Controller integrada, puede volver a configurar el tipo de implementación y cambiar a vCenter Server con una instancia de Platform Services Controller externa.

Consulte Reconfigurar una instancia de vCenter Server independiente con una instancia de Platform Services Controller integrada en un vCenter Server con una instancia de Platform Services Controller externa.

Platform Services Controller y vCenter Server con una instancia de Platform Services Controller externa

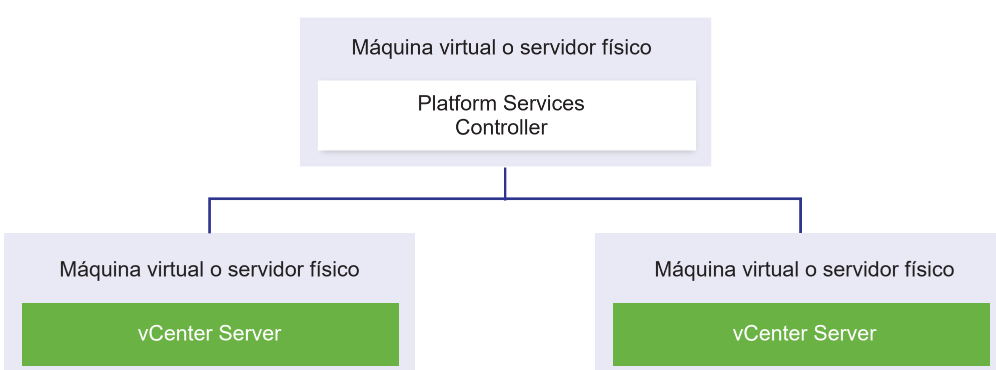
Cuando implementa o instala una instancia de Platform Services Controller, puede crear un dominio de vCenter Single Sign-On o unirse a un dominio de vCenter Single Sign-On existente. Las instancias de Platform Services Controller que se unieron replican sus datos de infraestructura, como la información de autenticación y licencias, y puede abarcar varios sitios de vCenter Single Sign-On. Para obtener información, consulte Comprender los sitios, nombres de dominio y dominios de vSphere.

Para obtener información sobre cómo administrar los servicios de Platform Services Controller, consulte *Administrar Platform Services Controller*.

Puede registrar varias instancias de vCenter Server con una instancia común externa de Platform Services Controller. Las instancias de vCenter Server asumen el sitio de vCenter Single Sign-On de la instancia de Platform Services Controller con la que están registradas. Todas las instancias de vCenter Server que están registradas con una instancia común o con diferentes instancias unidas de Platform Services Controller se conectan en el modo Enhanced Linked Mode.

Consulte Descripción general del modo vinculado mejorado.

Figura 1-3. Ejemplo de dos instancias de vCenter Server con una instancia común externa de Platform Services Controller



La instalación de vCenter Server con una instancia externa de Platform Services Controller posee las siguientes desventajas:

- La conexión entre vCenter Server y Platform Services Controller puede tener problemas de conectividad y de resolución de nombres.
- Si instala vCenter Server en máquinas virtuales o servidores físicos con Windows, necesitará más licencias de Microsoft Windows.
- Deberá administrar más máquinas virtuales o servidores físicos.

Para obtener información sobre los máximos de Platform Services Controller y vCenter Server, consulte la documentación de *Máximos de configuración*.

Para obtener información acerca de las topologías de implementación y la alta disponibilidad de Platform Services Controller, consulte Topologías de implementación con instancias de Platform Services Controller externas y alta disponibilidad.

Para obtener información sobre cómo configurar vCenter Server Appliance con una instancia externa de Platform Services Controller en la configuración de alta disponibilidad de vCenter, consulte *Disponibilidad de vSphere*.

Entorno de sistema operativo mixto

Una instancia de vCenter Server instalada en Windows puede registrarse con una instancia de Platform Services Controller instalada en Windows o un dispositivo de Platform Services Controller. Una instancia de vCenter Server Appliance puede registrarse con una instancia de Platform Services Controller instalada en Windows o con un dispositivo de Platform Services Controller. Tanto vCenter Server como vCenter Server Appliance pueden registrarse con la misma instancia de Platform Services Controller.

Figura 1-4. Ejemplo de un entorno de sistema operativo mixto con una instancia de Platform Services Controller externa en Windows

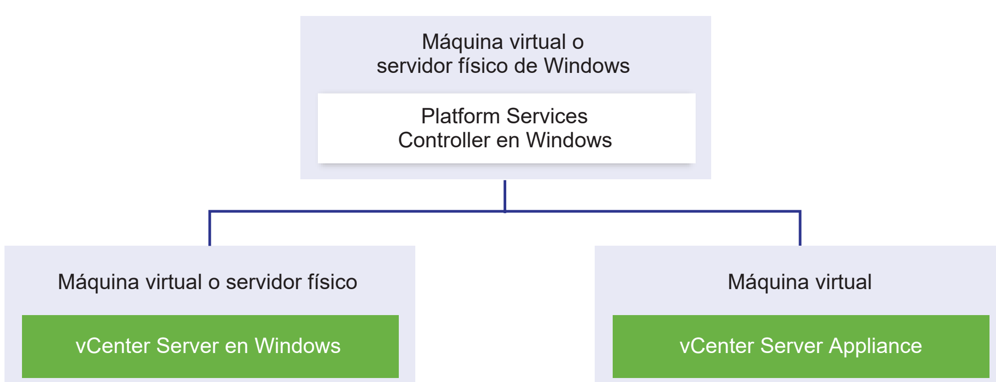
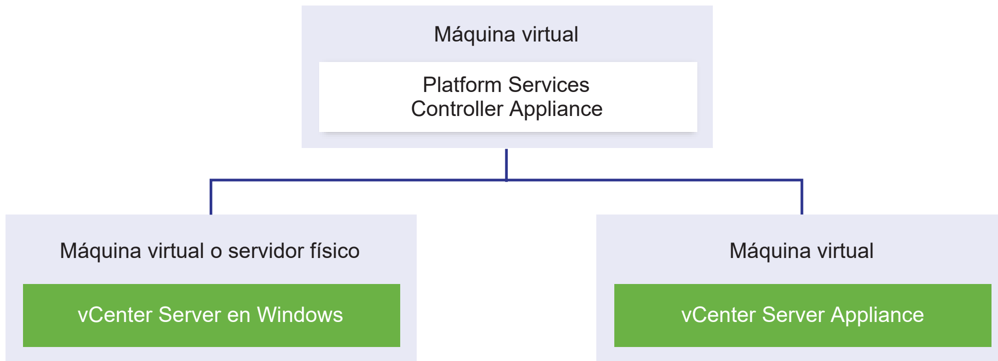


Figura 1-5. Ejemplo de un entorno de sistema operativo mixto con una aplicación de Platform Services Controller externa



Nota Para garantizar la capacidad de administración y mantenimiento, use solamente dispositivos o instalaciones para Windows de vCenter Server y Platform Services Controller.

Comprender los sitios, nombres de dominio y dominios de vSphere

Cada Platform Services Controller está asociado con un dominio de vCenter Single Sign-On. El valor predeterminado del nombre de dominio es vsphere.local, pero puede cambiarlo durante la instalación de la primera instancia de Platform Services Controller. El dominio determina el espacio de autenticación local. Puede dividir un dominio en varios sitios, y asignar cada instancia de Platform Services Controller y vCenter Server a un sitio. Los sitios son construcciones lógicas, pero generalmente corresponden a la ubicación geográfica.

Dominio de Platform Services Controller

Cuando instale una instancia de Platform Services Controller, se le solicitará que cree un dominio de vCenter Single Sign-On o que se una a un dominio existente.

VMware Directory Service (vmdir) usa el nombre del dominio para todas las estructuras internas del Protocolo Simplificado de Acceso a Directorios (LDAP).

Con vSphere 6.0 y posterior, puede dar a su dominio de vSphere un nombre único. Para evitar conflictos de autenticación, use un nombre que OpenLDAP, Microsoft Active Directory y otros servicios de directorio no usen.

Nota No puede cambiar el dominio al que pertenece una instancia de Platform Services Controller o vCenter Server.

Si está actualizando desde vSphere 5.5, el nombre del dominio de vSphere sigue siendo el predeterminado (vsphere.local). Para todas las versiones de vSphere, no puede cambiar el nombre de un dominio.

Después de especificar el nombre para el dominio, puede agregar usuarios y grupos. Normalmente es mejor agregar un origen de identidad de Active Directory o LDAP, y permitir a los usuarios y grupos de dicho origen que autentiquen. También puede agregar al dominio instancias de vCenter Server o Platform Services Controller, u otros productos VMware, como vRealize Operations.

Sitios de Platform Services Controller

Puede organizar los dominios de Platform Services Controller en sitios lógicos. Un sitio de VMware Directory Service es un contenedor lógico para agrupar instancias de Platform Services Controller dentro de un dominio de vCenter Single Sign-On.

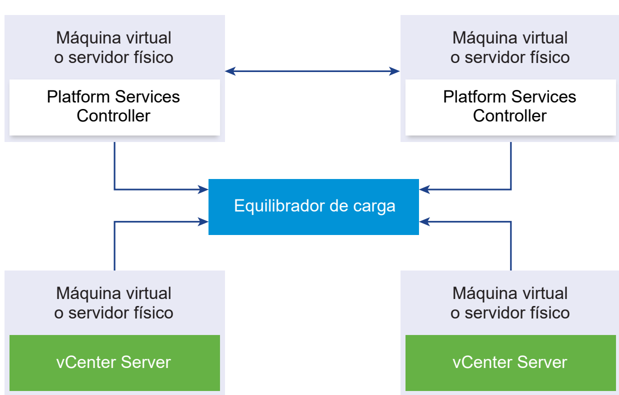
Se le pedirá el nombre de sitio al instalar o actualizar una instancia de Platform Services Controller. Consulte la documentación de *Instalar y configurar vSphere*.

Topologías de implementación con instancias de Platform Services Controller externas y alta disponibilidad

Para garantizar la alta disponibilidad de Platform Services Controller en las implementaciones externas, es necesario instalar o implementar al menos dos instancias unidas de Platform Services Controller en el dominio de vCenter Single Sign-On. Si se utiliza un equilibrador de carga de terceros, es posible garantizar una conmutación por error automática sin tiempo de inactividad.

Platform Services Controller con un equilibrador de carga

Figura 1-6. Ejemplo de un par con carga equilibrada de instancias de Platform Services Controller



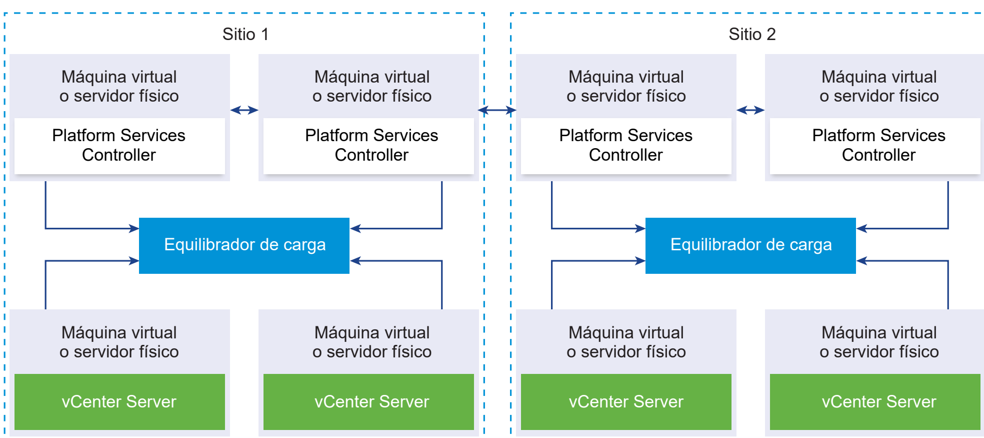
Es posible utilizar un equilibrador de carga de terceros por sitio para configurar la alta disponibilidad de Platform Services Controller con conmutación por error automática para ese sitio. Para obtener información sobre la cantidad máxima de instancias de Platform Services Controller detrás de un equilibrador de carga, consulte la documentación de *Máximos de configuración*.

Importante Para configurar la alta disponibilidad de Platform Services Controller detrás de un equilibrador de carga, las instancias de Platform Services Controller deben estar en el mismo tipo de sistema operativo. No se admiten las instancias de Platform Services Controller detrás de un equilibrador de carga en sistemas operativos combinados.

Las instancias de vCenter Server se conectan al equilibrador de carga. Cuando una instancia de Platform Services Controller deja de responder, el equilibrador de carga distribuye automáticamente la carga entre las otras instancias de Platform Services Controller en funcionamiento sin producir tiempo de inactividad.

Platform Services Controller con equilibradores de carga en sitios de vCenter Single Sign-On

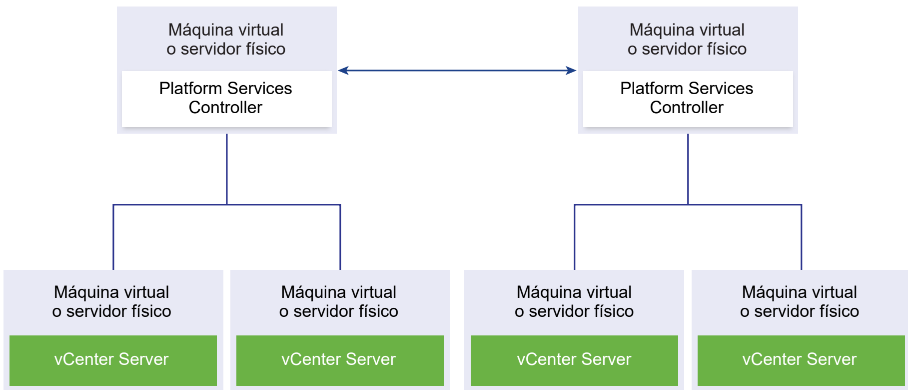
Figura 1-7. Ejemplo de dos pares con carga equilibrada de instancias de Platform Services Controller en dos sitios



El dominio de vCenter Single Sign-On puede abarcar varios sitios. Para garantizar la alta disponibilidad de Platform Services Controller con conmutación por error automática en todo el dominio, es necesario configurar un equilibrador de carga separado en cada sitio.

Platform Services Controller sin equilibrador de carga

Figura 1-8. Ejemplo de dos instancias unidas de Platform Services Controller sin ningún equilibrador de carga



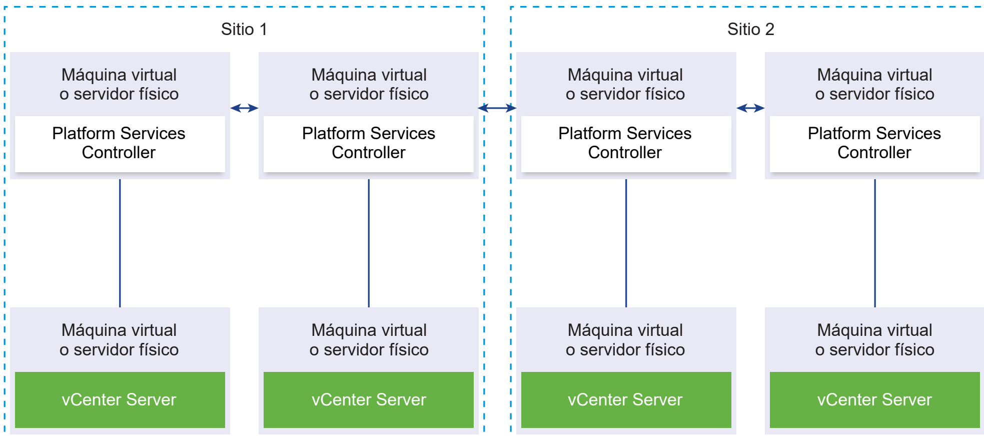
Cuando se unen dos o más instancias de Platform Services Controller en un mismo sitio sin ningún equilibrador de carga, se debe configurar la alta disponibilidad de Platform Services Controller con una conmutación por error manual para ese sitio.

Cuando una instancia de Platform Services Controller deja de responder, se deben conmutar manualmente las instancias de vCenter Server que están registradas en ella. Para conmutar las instancias, es necesario redirigirlas a otras instancias funcionales de Platform Services Controller dentro del mismo sitio. Consulte Redirigir vCenter Server a otra instancia de Platform Services Controller externa.

Nota Si su dominio de vCenter Single Sign-On incluye tres o más instancias de Platform Services Controller, puede crear manualmente una topología de anillo. Una topología de anillo garantiza la confiabilidad de Platform Services Controller cuando se produce un error en una de las instancias. Para crear una topología de anillo, ejecute el comando `/usr/lib/vmware-vmdir/bin/vdcrepadmin -f createagreement` en la primera y la última instancia de Platform Services Controller que implementó.

Platform Services Controller sin ningún equilibrador de carga en sitios de vCenter Single Sign-On

Figura 1-9. Ejemplo de dos pares unidos de instancias de Platform Services Controller en dos sitios sin equilibrador de carga



El dominio de vCenter Single Sign-On puede abarcar varios sitios. Cuando no existe ningún equilibrador de carga disponible, es posible redirigir manualmente vCenter Server de una instancia con errores a una instancia en funcionamiento de Platform Services Controller dentro del mismo sitio. Consulte Redirigir vCenter Server a otra instancia de Platform Services Controller externa.

Importante No se permite redirigir vCenter Server entre sitios y dominios. Si ninguna instancia funcional de Platform Services Controller está disponible en el sitio, debe implementar o instalar una nueva instancia de Platform Services Controller en este sitio. Esta nueva instancia de Platform Services Controller se convierte en el partner de replicación de la instancia de Platform Services Controller existente.

vCenter Enhanced Linked Mode

vCenter Enhanced Linked Mode permite iniciar sesión en cualquier instancia única de vCenter Server Appliance o vCenter Server, y ver y administrar los inventarios de todos los sistemas vCenter Server en el grupo.

A continuación se presentan los valores de configuración máximos de vCenter Enhanced Linked Mode:

- Para vCenter Server Appliance con implementaciones integradas de Platform Services Controller, puede unirse a hasta 15 nodos en un dominio de vSphere Single Sign-On.
- Para vCenter Server con instalaciones externas de Platform Services Controller, puede unirse a hasta 10 instancias externas de Platform Services Controller y 15 sistemas vCenter Server en un único dominio de vSphere Single Sign-On.

Puede crear un grupo de vCenter Enhanced Linked Mode únicamente durante la implementación de vCenter Server Appliance o la instalación de vCenter Server. No puede crear un grupo de vCenter Enhanced Linked Mode después de instalar vCenter Server ni después de implementar vCenter Server Appliance.

vCenter Embedded Linked Mode para vCenter Server Appliance con instancia integrada de Platform Services Controller

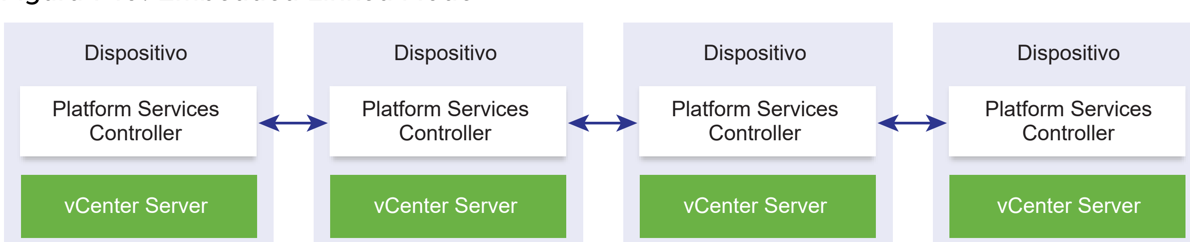
vCenter Embedded Linked Mode es el soporte de modo vinculado mejorado para vCenter Server Appliance con una instancia integrada de Platform Services Controller.

Con vCenter Embedded Linked Mode, puede conectar una instancia de vCenter Server Appliance con una instancia integrada de Platform Services Controller para formar un dominio. vCenter Embedded Linked Mode no es compatible con las instalaciones vCenter Server en Windows. vCenter Embedded Linked Mode es compatible a partir de vSphere 6.5 Update 2 y adecuado para la mayoría de las implementaciones.

Otras características de vCenter Embedded Linked Mode son:

- No se utiliza una instancia externa de Platform Services Controller, con lo que se obtiene una arquitectura de dominio más simple que una implementación externa con el modo vinculado mejorado.
- El proceso de copia de seguridad y restauración es simple. Para obtener más información, consulte "Restauración y copia de seguridad de vCenter Server Appliance basadas en archivos".
- El proceso de HA es simple, ya que no se necesitan equilibradores de carga.
- Es posible vincular hasta 15 instancias de vCenter Server Appliance mediante vCenter Embedded Linked Mode y mostrarlas en una sola vista de inventario.
- Para un clúster de vCenter High Availability (vCenter HA), tres nodos se consideran un nodo lógico de vCenter Server. Consulte "Descripción general de la arquitectura de vCenter" en *Disponibilidad de vSphere* para obtener un resumen de la arquitectura de vCenter HA. Un clúster de vCenter HA necesita una única licencia estándar de vCenter Server.

Figura 1-10. Embedded Linked Mode



Nota Embedded Linked Mode no es compatible con las instalaciones vCenter Server en Windows.

Embedded Linked Mode con replicación de solo lectura

Si una instancia de vCenter High Availability (vCenter HA) está conectada a otra instancia de vCenter Server que tiene habilitado Embedded Linked Mode, y la conmutación por error de vCenter HA se produce en el nodo pasivo y no puede comunicarse con su partner de replicación en el otro nodo de vCenter Server, la réplica en el nodo de vCenter HA entra en modo de solo lectura.

Unirse a un dominio de vCenter Embedded Linked Mode

Puede unir una instancia de vCenter Server con una instancia integrada de Platform Services Controller a otro nodo integrado durante la implementación de vCenter Server Appliance.

Por ejemplo, supongamos que tiene dos instancias de vCenter Server con sistemas Platform Services Controller integrados.

Si planea implementar las instancias de vCenter Server Appliance con el instalador de interfaz de usuario:

1. Para el dispositivo 1, implemente vCenter Server Appliance como una instancia en el host ESXi 1. Sincronice la configuración de hora con el host ESXi 1.
2. Para el dispositivo 2, implemente vCenter Server Appliance como una instancia en el host ESXi 1 y ajuste la configuración de hora para que el dispositivo 2 se sincronice con el host ESXi 1. En la etapa 2, seleccione unir el servidor vCenter Single Sign-On del dispositivo implementado en la máquina 1. Para obtener instrucciones específicas, consulte Etapa 2 - Configure la instancia de vCenter Server Appliance recién implementada con Platform Services Controller integrado.

Si planea implementar las instancias de vCenter Server Appliance con la CLI:

1. Establezca los parámetros de la plantilla de configuración JSON `embedded_vCSA_on_VC.json` (o `embedded_vCSA_on_ESXi.json`) para el dispositivo 1 como una instancia en el host ESXi 1. Consulte Preparar el archivo de configuración JSON para la implementación de CLI para obtener instrucciones específicas sobre la preparación del archivo de configuración JSON.
2. Implemente el dispositivo 1 mediante el comando `vcsa-cli-installer`. Consulte Implementar una instancia de vCenter Server Appliance o un dispositivo de Platform Services Controller mediante la CLI para obtener instrucciones.
3. Establezca los parámetros de la plantilla de configuración JSON `embedded_vCSA_replication_on_VC.json` (o `embedded_vCSA_replication_on_ESXi.json`) para el dispositivo 2 como una instancia en el host ESXi 1. Introduzca el nombre de host del primer nodo integrado en el campo `replication_partner_hostname` de la sección `sso`.
4. Implemente el dispositivo 2 mediante el comando `vcsa-cli-installer` utilizando el archivo `embedded_vCSA_replication_on_VC.json` (o `embedded_vCSA_replication_on_ESXi.json`).

Descripción general del modo vinculado mejorado

El modo vinculado mejorado conecta varios sistemas vCenter Server por medio de una instancia de Platform Services Controller o más.

El modo vinculado mejorado permite ver y buscar contenido en todos los sistemas vCenter Server vinculados y replicar roles, permisos, licencias, directivas y etiquetas.

Cuando instala vCenter Server o implementa vCenter Server Appliance con una instancia de Platform Services Controller externa, primero debe instalar Platform Services Controller. Durante la instalación de Platform Services Controller, puede determinar si desea crear un dominio de vCenter Single Sign-On o unirse a un dominio existente. Puede seleccionar unirse a un dominio existente de vCenter Single Sign-On si ya instaló o implementó una instancia de Platform Services Controller, y si creó un dominio de vCenter Single Sign-On. Cuando se une a un dominio de vCenter Single Sign-On existente, se replican los datos de infraestructura entre la instancia de Platform Services Controller existente y la instancia de Platform Services Controller nueva.

Con el modo vinculado mejorado, puede conectar no solo sistemas vCenter Server que ejecuten Windows, sino también una gran cantidad de instancias de vCenter Server Appliance. También puede tener un entorno en el que haya varios sistemas vCenter Server y vCenter Server Appliance vinculados juntos.

Si instala vCenter Server con una instancia de Platform Services Controller externa, primero debe implementar Platform Services Controller en una de las máquinas virtuales o en el servidor físico y, a continuación, debe implementar vCenter Server en otras máquinas virtuales o en otro servidor físico. Mientras instala vCenter Server, debe seleccionar una instancia de Platform Services Controller externa existente. No se puede seleccionar una instancia de Platform Services Controller existente que forme parte de una instalación integrada. Para obtener más información sobre las topologías admitidas, consulte Tipos de implementación de vCenter Server y Platform Services Controller.

Acerca de los modos de evaluación y con licencia de ESXi

Puede utilizar el modo de evaluación para explorar el conjunto completo de funciones para los hosts ESXi. El modo de evaluación proporciona un conjunto de funciones equivalente a una licencia de vSphere Enterprise Plus. Antes de que finalice el modo de evaluación, debe asignar a sus hosts una licencia que admita todas las funciones en uso.

Por ejemplo, en el modo de evaluación, puede utilizar la tecnología vSphere vMotion, la función vSphere HA, la característica vSphere DRS y otras características. Si desea continuar utilizando estas funciones, debe asignar una licencia que las admita.

La versión de los hosts ESXi Installable se instala siempre en el modo de evaluación. ESXi Embedded se ofrece preinstalado en el dispositivo de almacenamiento interno por parte de cada proveedor de hardware. Podría estar en el modo de evaluación o con licencia previa.

El período de evaluación es de 60 días y comienza cuando se enciende el host ESXi. En cualquier momento durante el período de evaluación de 60 días, se puede realizar la conversión de un modo con licencia a un modo de evaluación. El tiempo disponible en el modo de evaluación se resta del tiempo ya consumido.

Por ejemplo, supongamos que se utiliza un host ESXi en el modo de evaluación durante 20 días y, a continuación, se asigna una clave de licencia de vSphere Standard Edition al host. Si se vuelve a establecer el host en el modo de evaluación, se podrá explorar el conjunto completo de funciones para el host durante el período de evaluación restante de 40 días.

Para obtener información sobre la administración de licencias para los hosts ESXi, consulte la documentación *Administrar vCenter Server y hosts*.

Instalar y configurar ESXi

2

Se puede instalar y configurar ESXi en el hardware físico de modo que actúe como plataforma para las máquinas virtuales.

Este capítulo incluye los siguientes temas:

Requisitos de ESXi

Para instalar o actualizar ESXi, el sistema debe cumplir con requisitos de hardware y software específicos.

Requisitos de hardware de ESXi

Asegúrese de que el host cumpla los requisitos de hardware mínimos de ESXi6.5.

Recursos de hardware y del sistema

Para instalar o actualizar ESXi, los recursos de hardware y del sistema deben cumplir los siguientes requisitos:

- Plataforma de servidores compatible. Para obtener una lista de plataformas compatibles, consulte la *Guía de compatibilidad de VMware* en http://www.vmware.com/resources/compatibility.
- ESXi 6.5 requiere un equipo host con al menos dos núcleos de CPU.
- ESXi 6.5 admite procesadores x86 de 64 bits desde septiembre de 2006. Esto incluye una amplia gama de procesadores de varios núcleos. Para obtener una lista completa de procesadores compatibles, consulte la guía de compatibilidad de VMware en http://www.vmware.com/resources/compatibility.
- ESXi 6.5 requiere que el bit NX/XD esté habilitado para la CPU en el BIOS.

- ESXi 6.5 requiere un mínimo de 4 GB de RAM física. Se recomienda proporcionar al menos 8 GB de RAM para ejecutar máquinas virtuales en entornos de producción típicos.
- Para admitir máquinas virtuales de 64 bits, se debe habilitar la compatibilidad para virtualización de (Intel VT-x o RVI AMD) en CPU x64.
- Una o más controladoras Gigabit o Ethernet más rápidas. Para obtener una lista de modelos de adaptadores de red compatibles, consulte la *Guía de compatibilidad de VMware* en http://www.vmware.com/resources/compatibility.
- Disco SCSI o un LUN RAID local que no sea de red con espacio sin particionar para las máquinas virtuales.
- Para la serie ATA (SATA), un disco conectado a través de controladoras SAS compatibles o controladoras SATA integradas compatibles. Los discos SATA se consideran remotos, no locales. Estos discos no se usan como una partición desde cero de forma predeterminada, ya que se consideran remotos.

  Nota No puede conectar un dispositivo CD-ROM SATA a una máquina virtual en un host ESXi 6.5. Para usar el dispositivo CD-ROM SATA, debe usar el modo de emulación IDE.

Sistemas de almacenamiento

Para obtener una lista de sistemas de almacenamiento compatibles, consulte la *Guía de compatibilidad de VMware* en http://www.vmware.com/resources/compatibility. Para obtener información sobre software Fibre Channel over Ethernet (FCoE), consulte Instalar y arrancar ESXi con FCoE de software.

Requisitos de arranque de ESXi

vSphere 6.5 admite el arranque de hosts ESXi desde la Unified Extensible Firmware Interface (UEFI). Con la UEFI, puede arrancar sistemas desde unidades de disco duro, unidades de CD-ROM o medios USB.

A partir de vSphere 6.5, VMware Auto Deploy admite el arranque de redes y el aprovisionamiento de hosts ESXi mediante UEFI.

ESXi puede arrancar desde un disco con más de 2 TB siempre que el firmware del sistema y el firmware en cualquier tarjeta adicional que esté usando lo admitan. Consulte la documentación del proveedor.

Requisitos de almacenamiento para la instalación o actualización de ESXi 6.5

La instalación de ESXi 6.5 o la actualización a ESXi 6.5 requiere un dispositivo de arranque de al menos 1 GB. Cuando se arranca desde un disco local, SAN o LUN iSCSI, se requiere un disco de 5,2 GB para permitir la creación del volumen de VMFS y la partición temporal de 4 GB en el dispositivo de arranque. Si se usa un disco o LUN de menor tamaño, el instalador intenta

asignar una región temporal en un disco local separado. Si un disco local no se puede encontrar, la partición desde cero, `/scratch`, está en el ramdisk de host ESXi, vinculado a `/tmp/scratch`. Puede volver a configurar `/scratch` para que use un disco o LUN separado. Para obtener el mejor rendimiento y optimización de la memoria, no deje `/scratch` en el ramdisk de host ESXi.

Para volver a configurar `/scratch`, consulte Establecer la partición desde cero de vSphere Web Client.

Debido a la sensibilidad de E/S de los dispositivos USB y SD, el instalador no crea una partición desde cero en estos dispositivos. Cuando se realiza una instalación o actualización en dispositivos USB o SD, el instalador intenta asignar una región desde cero en un disco o un almacén de datos local disponible. Si no se encuentra un disco o un almacén de datos local, `/scratch` está ubicado en el ramdisk. Después de la instalación o la actualización, debe volver a configurar `/scratch` para usar un almacén de datos persistente. Aunque es suficiente un dispositivo USB o SD de 1 GB para una instalación mínima, debe usar un dispositivo de 4 GB o más grande. El espacio adicional se utiliza para una partición de volcado de memoria del núcleo ampliada en el disco USB/SD. Use una unidad flash USB de alta calidad de 16 GB o mayor de manera que las celdas flash adicionales puedan prolongar la vida útil de los medios de arranque, pero es suficiente con unidades de alta calidad de 4 GB o mayores para mantener la partición de volcado del núcleo ampliada. Consulte el artículo de la base de conocimientos http://kb.vmware.com/kb/2004784.

En instalaciones de Auto Deploy, el instalador intenta asignar una región temporal en un disco o un almacén de datos local disponible. Si no se encuentra un disco o un almacén de datos local, `/scratch` está ubicado en ramdisk. Debe volver a configurar `/scratch` para usar un almacén de datos persistente después de la instalación.

Para entornos que arrancan desde un SAN o utilizan Auto Deploy, tiene que asignar un LUN separado para cada host ESXi. Puede localizar conjuntamente las regiones temporales para muchos hosts ESXi en un solo LUN. La cantidad de hosts asignados a un solo LUN deben sopesarse con respecto al tamaño del LUN y el comportamiento de E/S de las máquinas virtuales.

Modelos de servidores de administración remota compatibles y versiones de firmware

Puede utilizar aplicaciones de administración remota para instalar o actualizar ESXi o para administrar hosts de forma remota.

Tabla 2-1. Modelos de servidores de administración remota compatibles y versiones de firmware mínimas

Modelo de servidor de administración remota	Versión de firmware	Java
Dell DRAC 7	1.30.30 (compilación 43)	1.7.0_60-b19
Dell DRAC 6	1.54 (compilación 15), 1.70 (compilación 21)	1.6.0_24
Dell DRAC 5	1.0, 1.45, 1.51	1.6.0_20,1.6.0_203
Dell DRAC 4	1.75	1.6.0_23

Tabla 2-1. Modelos de servidores de administración remota compatibles y versiones de firmware mínimas (continuación)

Modelo de servidor de administración remota	Versión de firmware	Java
ILO HP	1.81, 1.92	1.6.0_22, 1.6.0_23
ILO HP 2	1.8, 1.81	1.6.0_20, 1.6.0_23
ILO HP 3	1.28	1.7.0_60-b19
ILO HP 4	1.13	1.7.0_60-b19
RSA IBM 2	1.03, 1.2	1.6.0_22

Recomendaciones para un rendimiento mejorado de ESXi

Para mejorar el rendimiento, instale o actualice ESXi en un sistema robusto con más RAM que el mínimo necesario y con varios discos físicos.

Para conocer los requisitos del sistema de ESXi, consulte Requisitos de hardware de ESXi.

Tabla 2-2. Recomendaciones para un mejor rendimiento

Elemento del sistema	Recomendación
RAM	Los hosts ESXi requieren más RAM que los servidores típicos. Proporcione al menos 8 GB de RAM para aprovechar al máximo las características de ESXi y ejecutar máquinas virtuales en entornos de producción típicos. Un host ESXi debe tener suficiente RAM para que funcionen máquinas virtuales simultáneas. Se proporcionan los siguientes ejemplos para ayudar a calcular la RAM que necesitan las máquinas virtuales que se ejecutan en el host ESXi. Para operar cuatro máquinas virtuales con Red Hat Enterprise Linux o Windows XP se requiere al menos 3 GB de RAM para rendimiento línea base. Esta cifra incluye aproximadamente 1.024 MB para las máquinas virtuales, 256 MB como mínimo para cada sistema operativo, según lo que recomiendan los proveedores. Para que funcionen estas cuatro máquinas virtuales con 512 MB de RAM, es necesario que los hosts ESXi tengan aproximadamente 4 GB de RAM, lo que incluye 2048 MB para las máquinas virtuales. Estos cálculos no tienen en cuenta los posibles ahorros de memoria derivados de usar memoria con sobrecarga variable para cada máquina virtual. Consulte *Administración de recursos de vSphere*.
Adaptadores Fast Ethernet dedicados para máquinas virtuales	Coloque la red de administración y las redes de máquinas virtuales en tarjetas de red físicas distintas. Las tarjetas Gigabit Ethernet dedicadas para máquinas virtuales, como adaptadores Intel PRO 1000, mejoran el rendimiento para máquinas virtuales con gran tráfico de red.
Ubicación del disco	Coloque todos los datos que usan las máquinas virtuales en discos físicos asignados específicamente a máquinas virtuales. El rendimiento es mejor cuando no coloca las máquinas virtuales en el disco que contiene la imagen de arranque de ESXi. Use discos físicos que sean lo bastante grandes para mantener imágenes del disco que usan todas las máquinas virtuales.
partición de VMFS5	El instalador de ESXi crea los volúmenes iniciales de VMFS en el primer disco local en blanco que se encuentra. Para agregar discos o modificar la configuración original, use vSphere Web Client. Esta práctica asegura que los sectores de arranque de las particiones estén alineados con 64K, lo que mejora el rendimiento del almacenamiento. **Nota** Para entornos únicamente de SAS, es posible que el instalador no formatee los discos. Para algunos discos SAS, no es posible identificar si los discos son locales o remotos. Después de la instalación, se puede usar vSphere Web Client para configurar VMFS.

Tabla 2-2. Recomendaciones para un mejor rendimiento (continuación)

Elemento del sistema	Recomendación
Procesadores	Los procesadores más rápidos mejoran el rendimiento de ESXi. Para ciertas cargas de trabajo, una mayor cantidad de memorias caché mejoran el rendimiento de ESXi.
Compatibilidad de hardware	Use dispositivos en el servidor que sean compatibles con controladores de ESXi 6.5. Consulte la *Guía de compatibilidad de hardware* en http://www.vmware.com/resources/compatibility.

Puertos de firewall entrantes y salientes para hosts de ESXi

vSphere Web Client y VMware Host Client permiten abrir y cerrar puertos de firewall para cada servicio o para admitir tráfico de las direcciones IP seleccionadas.

En la siguiente tabla, se muestran los firewalls para los servicios que se instalan de forma predeterminada. Si instala otros VIB en el host, es posible que estén disponibles otros puertos de firewall y servicios adicionales. La información es principalmente para los servicios que están visibles en vSphere Web Client, pero la tabla también incluye otros puertos.

Tabla 2-3. Conexiones de firewall entrantes

Puerto	Protocolo	Servicio	Descripción
5988	TCP	Servidor CIM	Servidor para CIM (Common Information Model).
5989	TCP	Servidor CIM seguro	Servidor seguro para CIM.
427	TCP, UDP	CIM SLP	El cliente CIM usa el protocolo de ubicación de servicios, versión 2 (SLPv2), para buscar servidores CIM.
546		DHCPv6	Cliente DHCP para IPv6.
8301, 8302	UDP	DVSSync	Se usan puertos de DVSSync para sincronizar los estados de los puertos virtuales distribuidos entre los hosts que tienen habilitada la opción de grabación/reproducción de VMware FT. Solo los hosts que ejecutan máquinas virtuales principales o de copia de seguridad deben tener abiertos estos puertos. En los hosts que no usan VMware FT, no es necesario que estos puertos estén abiertos.
902	TCP	NFC	Network File Copy (NFC) proporciona un servicio de FTP basado en los tipos de archivos para los componentes de vSphere. Como opción predeterminada, ESXi usa NFC para las operaciones, como la copia y la transferencia de datos entre áreas de almacenamiento de datos.
12345, 23451	UDP	Servicio de clústeres de vSAN	Servicio de directorio de membresía y supervisión de clústeres de VMware vSAN. Usa multidifusión IP basada en UDP para establecer los miembros del clúster y distribuir los metadatos de vSAN a todos los miembros del clúster. Si se deshabilita, vSAN no funciona.
68	UDP	Cliente DHCP	Cliente DHCP para IPv4.
53	UDP	Cliente DNS	Cliente DNS.

Tabla 2-3. Conexiones de firewall entrantes (continuación)

Puerto	Protocolo	Servicio	Descripción
8200, 8100, 8300	TCP, UDP	Fault Tolerance	Tráfico entre hosts para vSphere Fault Tolerance (FT).
6999	UDP	Servicio de enrutador lógico distribuido de NSX	Servicio de enrutador virtual distribuido de NSX. El puerto de firewall asociado con este servicio se abre cuando se instalan los VIB de NSX y se crea el módulo de VDR. Si no hay instancias de VDR asociadas con el host, no es necesario que el puerto esté abierto. En versiones anteriores del producto, este servicio se llamaba Enrutador lógico distribuido de NSX.
2233	TCP	Transporte de vSAN	Transporte fiable de datagramas de vSAN. Emplea TCP y se utiliza para E/S de almacenamiento de vSAN. Si se deshabilita, vSAN no funciona.
161	UDP	Servidor SNMP	Permite que el host se conecte a un servidor SNMP.
22	TCP	Servidor SSH	Es necesario para el acceso a SSH.
8000	TCP	vMotion	Es necesario para la migración de máquinas virtuales con vMotion. Los hosts ESXi escuchan en el puerto 8000 para las conexiones TCP de los hosts ESXi remotos para el tráfico de vMotion.
902, 443	TCP	vSphere Web Client	Conexiones de clientes
8080	TCP	vsanvp	Proveedor del proveedor VASA de vSAN. Lo utiliza el servicio de administración de almacenamiento (SMS) que forma parte de vCenter para acceder a la información sobre cumplimiento de normas, funcionalidades y perfiles de almacenamiento de vSAN. Si se deshabilita, la administración del almacenamiento basada en perfiles (SPBM) de vSAN no funciona.
80	TCP	vSphere Web Access	Página principal, con vínculos de descarga para diferentes interfaces.
5900-5964	TCP	Protocolo RFB	
80, 9000	TCP	vSphere Update Manager	
9080	TCP	Servicio de filtro de E/S	Utilizado por la función de almacenamiento de filtros de E/S

Tabla 2-4. Conexiones de firewall salientes

Puerto	Protocolo	Servicio	Descripción
427	TCP, UDP	CIM SLP	El cliente CIM usa el protocolo de ubicación de servicios, versión 2 (SLPv2), para buscar servidores CIM.
547	TCP, UDP	DHCPv6	Cliente DHCP para IPv6.

Tabla 2-4. Conexiones de firewall salientes (continuación)

Puerto	Protocolo	Servicio	Descripción
8301, 8302	UDP	DVSSync	Se usan puertos de DVSSync para sincronizar los estados de los puertos virtuales distribuidos entre los hosts que tienen habilitada la opción de grabación/reproducción de VMware FT. Solo los hosts que ejecutan máquinas virtuales principales o de copia de seguridad deben tener abiertos estos puertos. En los hosts que no usan VMware FT, no es necesario que estos puertos estén abiertos.
44046, 31031	TCP	HBR	Se usa para tráfico de replicación continuo de vSphere Replication y VMware Site Recovery Manager.
902	TCP	NFC	Network File Copy (NFC) proporciona un servicio de FTP basado en los tipos de archivos para los componentes de vSphere. Como opción predeterminada, ESXi usa NFC para las operaciones, como la copia y la transferencia de datos entre áreas de almacenamiento de datos.
9	UDP	WOL	Utilizado por Wake-on-LAN.
12345 23451	UDP	Servicio de clústeres de vSAN	Servicio de directorio, membresía y supervisión de clústeres utilizado por vSAN.
68	UDP	Cliente DHCP	Cliente DHCP.
53	TCP, UDP	Cliente DNS	Cliente DNS.
80, 8200, 8100, 8300	TCP, UDP	Fault Tolerance	Es compatible con VMware Fault Tolerance.
3260	TCP	Cliente iSCSI de software	Es compatible con iSCSI de software.
6999	UDP	Servicio de enrutador lógico distribuido de NSX	El puerto de firewall asociado con este servicio se abre cuando se instalan los VIB de NSX y se crea el módulo de VDR. Si no hay instancias de VDR asociadas con el host, no es necesario que el puerto esté abierto.
5671	TCP	rabbitmqproxy	Un proxy que se ejecuta en el host ESXi. Este proxy permite que las aplicaciones que se ejecutan dentro de máquinas virtuales se comuniquen con los agentes de AMQP que se ejecutan en el dominio de la red de vCenter. No es necesario que la máquina virtual esté en la red (es decir, no se requiere la NIC). Asegúrese de que las direcciones IP de conexión salientes incluyen al menos los agentes en uso o futuros. Los agentes se pueden añadir más adelante para escalar verticalmente.
2233	TCP	Transporte de vSAN	Se utiliza para tráfico de RDT (comunicación de punto a punto de Unicast) entre nodos de vSAN.
8000	TCP	vMotion	Es necesario para la migración de máquinas virtuales con vMotion.

Tabla 2-4. Conexiones de firewall salientes (continuación)

Puerto	Protocolo	Servicio	Descripción
902	UDP	VMware vCenter Agent	vCenter Server Agent.
8080	TCP	vsanvp	Se utiliza para el tráfico de proveedores de vSAN.

Tabla 2-5. Puertos de firewall para los servicios que no están visibles en la UI de manera predeterminada

Puerto	Protocolo	Servicio	Comentario
5900-5964	TCP	Protocolo RFB	El protocolo RFB es un protocolo simple para acceder de manera remota a las interfaces gráficas de usuario.
8889	TCP	Daemon de OpenWSMAN	Web Services Management (WS-Management) es un estándar abierto de DMTF para la administración de servidores, dispositivos, aplicaciones y servicios web.

Espacio libre necesario para registro del sistema

Si utilizó Auto Deploy para instalar el host ESXi6.5, o bien si configuró un directorio de registro separado de la ubicación predeterminada en un directorio totalmente nuevo en el volumen de VMFS, es posible que deba cambiar su configuración de tamaño y rotación de registro actual para garantizar que el espacio disponible sea suficiente para el registro del sistema.

Todos los componentes de vSphere usan esta infraestructura. Los valores predeterminados para la capacidad de registros en esta infraestructura varían según la cantidad de almacenamiento disponible y cómo ha configurado el registro del sistema. Los hosts que se implementan con Auto Deploy almacenan registros en un disco RAM, lo que significa que hay poca cantidad de espacio disponible para registros.

Si su host se implementa con Auto Deploy, vuelva a configurar el almacenamiento de sus registros de una de estas formas:

- Redirija los registros a través de la red hacia un recopilador remoto.
- Redirija registros hacia un almacenamiento NAS o NFS.

Si redirige los registros hacia un almacenamiento no predeterminado, como NAS o NFS, es posible que también desee volver a configurar el dimensionamiento y las rotaciones de los registros para los hosts que están instalados en el disco.

No tiene que volver a configurar el almacenamiento de registros para hosts ESXi que utilizan la configuración predeterminada, que almacena registros en un directorio temporal en el volumen de VMFS. Para estos hosts, ESXi6.5 configura registros que se adapten de la mejor manera a cada instalación y proporciona suficiente espacio para alojar mensajes de registros.

Tabla 2-6. Configuración recomendada de tamaño y rotación mínima para registros hostd, vpxa y fdm

Registro	Tamaño máximo de archivo de registro	Cantidad de rotaciones que se debe mantener	Espacio de disco mínimo necesario
Agente de administración (hostd)	10 MB	10	100 MB
Agente VirtualCenter (vpxa)	5 MB	10	50 MB
Agente de vSphere HA (administrador de dominio de fallas, fdm)	5 MB	10	50 MB

Para obtener información sobre la configuración de un servidor de registro remoto, consulte Configurar Syslog en hosts ESXi.

Requisitos del sistema de VMware Host Client

Asegúrese de que su explorador sea compatible con VMware Host Client.

Los siguientes sistemas operativos invitados y las siguientes versiones de exploradores web son compatibles con VMware Host Client.

Exploradores compatibles	Mac OS	Windows	Linux
Google Chrome	75+	75+	75+
Mozilla Firefox	60+	60+	60+
Microsoft Edge	N/C	79+	N/C
Safari	9.0+	N/C	N/C

Preparativos para la instalación de ESXi

Antes de instalar ESXi, determine la opción de instalación más adecuada para el entorno y prepare el proceso de instalación.

Descarga del instalador de ESXi

Descargue el instalador de ESXi.

Requisitos previos

Cree una cuenta de VMware Customer Connect en https://my.vmware.com/web/vmware/.

Procedimiento

1 Inicie sesión en VMware Customer Connect.

2 Desplácese hasta **Productos y cuentas > Todos los productos**.

3. Busque VMware vSphere y haga clic en **Descargar producto**.
4. Seleccione una versión de VMware vSphere en el menú desplegable **Seleccionar versión**.
5. Seleccione una versión de VMware vSphere Hypervisor (ESXi) y haga clic en **IR A DESCARGAS**.
6. Descargue una imagen ISO de ESXi.
7. Confirme que md5sum sea correcto mediante una herramienta de suma de comprobación MD5.

Opciones para instalar ESXi

ESXi puede instalarse de varias maneras. Para garantizar que vSphere se implemente de la mejor manera, debe comprender las opciones en profundidad antes de comenzar la instalación.

Las instalaciones de ESXi están diseñadas para incluir distintos tamaños de implementación.

En base al método que elija, tendrá diferentes opciones disponibles para acceder a medios de instalación y arrancar el instalador.

Instalar ESXi de manera interactiva

Las instalaciones interactivas se recomiendan para las implementaciones pequeñas con menos de cinco hosts.

El instalador se arranca desde un CD o DVD, desde un dispositivo USB de arranque o mediante un arranque con PXE del instalador desde una ubicación de la red. Debe seguir las indicaciones del asistente de instalación para instalar ESXi en el disco. Consulte Instalar ESXi de forma interactiva.

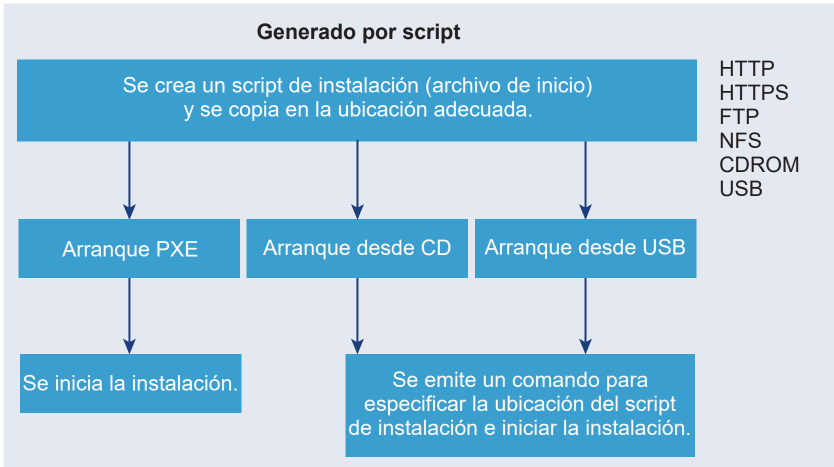
Instalación de ESXi generada por script

La ejecución de un script es una manera eficaz de implementar varios hosts ESXi mediante una instalación desatendida.

El script de instalación contiene los ajustes de configuración del host. Puede usar el script para configurar varios hosts con las mismas opciones. Consulte Instalar o actualizar hosts mediante un script.

El script de instalación debe almacenarse en una ubicación a la que el host pueda acceder mediante HTTP, HTTPS, FTP, NFS, CD-ROM o USB. Puede arrancar el instalador de ESXi mediante PXE o desde una unidad USB o de CD/DVD.

Figura 2-1. Instalación generada por script



Instalar ESXi con vSphere Auto Deploy

vSphere 5.x y versiones posteriores permiten instalar ESXi con vSphere Auto Deploy de varias formas.

vSphere Auto Deploy puede aprovisionar cientos de hosts físicos con el software ESXi. Se puede especificar la imagen que se implementará y los hosts que se aprovisionarán con esa imagen. Opcionalmente, puede especificar perfiles para aplicarlos a los hosts, una ubicación de vCenter Server (centro de datos, carpeta o clúster) y un paquete de scripts para cada host.

vCenter Server permite que las actualizaciones y las revisiones de ESXi estén disponibles para descarga a través de un perfil de imagen. La configuración del host se proporciona a través de un perfil de host. Puede crear perfiles de host mediante vSphere Web Client. Puede crear perfiles de imagen personalizados mediante vSphere ESXi Image Builder. Consulte Personalizar instalaciones con vSphere ESXi Image Builder y *Perfiles de host de vSphere*.

Al aprovisionar hosts mediante vSphere Auto Deploy, vCenter Server carga la imagen de ESXi directamente en la memoria del host. vSphere Auto Deploy no almacena el estado de ESXi en el disco host. El servidor de vSphere Auto Deploy continúa aprovisionando este host cada vez que arranca.

También puede utilizar vSphere Auto Deploy para instalar un host ESXi, así como configurar un perfil de host que haga que el host almacene la imagen y la configuración de ESXi en el disco local, en un disco remoto o en una unidad USB. Por tanto, el host ESXi arranca desde esta imagen local y vSphere Auto Deploy deja de aprovisionarlo. Este proceso es similar a realizar una instalación generada por scripts. Con una instalación generada por scripts, el script aprovisiona un host y el host arranca desde el disco. En este caso, vSphere Auto Deploy aprovisiona un host y después este arranca desde el disco. Para obtener más información, consulte Usar vSphere Auto Deploy para almacenamiento en caché sin estado e instalaciones con estado.

Opciones de medios para arrancar el instalador de ESXi

El instalador de ESXi debe ser accesible para el sistema en el que se va a instalar ESXi.

Los siguientes medios de arranque son compatibles con el instalador de ESXi:

- Arranque desde un CD/DVD. Consulte Descargar y grabar un CD or DVD de la imagen ISO del instalador de ESXi.
- Arranque desde una unidad flash USB. Consulte Formatear una unidad flash USB para arrancar la instalación o la actualización de ESXi.
- Arranque PXE desde la red. Arranque PXE del instalador de ESXi
- Arranque desde una ubicación remota mediante una aplicación de administración remota. Consulte Usar aplicaciones de administración remota

Descargar y grabar un CD or DVD de la imagen ISO del instalador de ESXi

Si no tiene un CD/DVD de instalación de ESXi, puede crear uno.

También puede crear una imagen ISO del instalador que incluya un script de instalación personalizado. Consulte Crear una imagen ISO de instalador con un script de instalación o actualización personalizado.

Procedimiento

1 Siga el procedimiento descrito en Descarga del instalador de ESXi.

2 Grabe la imagen ISO en un CD o DVD.

Formatear una unidad flash USB para arrancar la instalación o la actualización de ESXi

Puede formatear una unidad flash USB para arrancar la instalación o la actualización de ESXi.

En las instrucciones de este procedimiento se supone que la unidad flash USB se detecta como `/dev/sdb`.

Nota El archivo `ks.cfg` que contiene el script de instalación no puede estar ubicado en la misma unidad flash USB que se utiliza para arrancar la instalación o la actualización.

Requisitos previos

- Equipo Linux al que se acceda como superusuario
- Unidad flash USB que el equipo Linux pueda detectar
- La imagen ISO de ESXi, `VMware-VMvisor-Installer-`*`número_versión`*`-`*`número_compilación`*`.x86_64.iso`, que incluye el archivo `isolinux.cfg`
- Un paquete de Syslinux 3.86. Es posible que otras versiones no sean compatibles con ESXi.

Procedimiento

1 Arranque Linux, inicie sesión y entre en el modo de superusuario mediante un comando `su` o `sudo root`.

2 Si la unidad flash USB no se detecta como `/dev/sdb`, o si no conoce con certeza la forma en que se detecta la unidad flash USB, determine la manera en que se detecta.

   a Conecte la unidad flash USB.

   b En la línea de comandos, ejecute el comando para mostrar los mensajes de registro actuales.

   ```
   tail -f /var/log/messages
   ```

   Se mostrarán varios mensajes en los que se identifica la unidad flash USB con un formato similar al del siguiente mensaje.

   ```
   Oct 25 13:25:23 ubuntu kernel: [ 712.447080] sd 3:0:0:0: [sdb] Attached SCSI removable
   disk
   ```

   En este ejemplo, `sdb` identifica el dispositivo USB. Si el dispositivo se identifica de un modo diferente, use esa identificación en lugar de *sdb*.

3 Cree una tabla de particiones en el dispositivo flash USB.

```
/sbin/fdisk /dev/sdb
```

Como alternativa, introduzca **o** para crear una nueva tabla de particiones DOS vacía.

   a Introduzca `d` para eliminar las particiones hasta que no quede ninguna.

   b Introduzca `n` para crear una partición principal 1 que se extienda a todo el disco.

   c Introduzca `t` para configurar el tipo en una opción de configuración adecuada para el sistema de archivos FAT32, por ejemplo, **c**.

   d Introduzca `a` para establecer la marca de activo en la partición 1.

   e Introduzca `p` para imprimir la tabla de particiones.

   El resultado debe ser similar al siguiente mensaje.

   ```
   Disk /dev/sdb: 2004 MB, 2004877312 bytes 255 heads, 63 sectors/track, 243 cylinders
   Units = cylinders of 16065 * 512 = 8225280 bytes Device Boot Start End Blocks Id
   System /dev/sdb1 1 243 1951866 c W95 FAT32 (LBA)
   ```

   f Introduzca `w` para escribir la tabla de particiones y salir del programa.

4 Formatee la unidad flash USB con el sistema de archivos FAT32.

```
/sbin/mkfs.vfat -F 32 -n USB /dev/sdb1
```

5 Instale el cargador de arranque de Syslinux en la unidad flash USB.

Las ubicaciones del archivo ejecutable de Syslinux y del archivo `mbr.bin` pueden variar según las versiones de Syslinux. Los siguientes comandos están predeterminados.

```
/usr/bin/syslinux /dev/sdb1
cat /usr/lib/syslinux/mbr/mbr.bin > /dev/sdb
```

Por ejemplo, puede descargar una copia de `syslinux-3.86.zip`, descomprimir el archivo, compilar el código fuente de syslinux siguiendo sus instrucciones y, a continuación, si ejecuta la instalación de syslinux desde el directorio descargado, puede utilizar los siguientes comandos:

```
cd ~/Downloads/syslinux-3.86
.mtools/syslinux /dev/sdb1
cat mbr/mbr.bin > /dev/sdb
```

6 Cree un directorio de destino y monte la unidad flash USB allí.

```
mkdir /usbdisk
mount /dev/sdb1 /usbdisk
```

7 Cree un directorio de origen y monte la imagen ISO del instalador de ESXi allí.

```
mkdir /esxi_cdrom
mount -o loop VMware-VMvisor-Installer-version_number-build_number.x86_64.iso /esxi_cdrom
```

8 Copie el contenido de la imagen ISO en la unidad flash USB.

```
cp -r /esxi_cdrom/* /usbdisk
```

9 Cambie el nombre del archivo `isolinux.cfg` por `syslinux.cfg`.

```
mv /usbdisk/isolinux.cfg /usbdisk/syslinux.cfg
```

10 En el archivo `usbdisk/syslinux.cfg`, edite la línea de `APPEND -c boot.cfg` como `APPEND -c boot.cfg -p 1` para asegurarse de que el cargador de arranque lea los archivos de la primera partición, que creó en el paso 3. El número de partición puede ser diferente según el diseño del dispositivo USB.

11 Desmonte la unidad flash USB.

```
umount /usbdisk
```

12 Desmonte la imagen ISO del instalador.

```
umount /esxi_cdrom
```

Resultados

Puede utilizar la unidad flash USB para arrancar el instalador de ESXi.

Crear una unidad flash USB para almacenar el script de instalación o actualización de ESXi

Puede utilizar una unidad flash USB para almacenar el script de instalación o actualización de ESXi que se va a utilizar para la instalación o actualización por script de ESXi.

Si existen varias unidades flash USB en el equipo de instalación, el software de instalación busca el script de instalación o actualización en todas las unidades flash USB que estén conectadas.

En las instrucciones de este procedimiento se supone que la unidad flash USB se detecta como `/dev/sdb`.

Nota No almacene el archivo `ks` que contiene el script de instalación o actualización en la misma unidad flash USB que se utiliza para arrancar la instalación o la actualización.

Requisitos previos

- Equipo Linux
- Script de instalación o actualización de ESXi, el archivo kickstart `ks.cfg`
- Unidad flash USB

Procedimiento

1. Conecte la unidad flash USB a un equipo Linux con acceso al script de instalación o actualización.
2. Cree una tabla de particiones.

   `/sbin/fdisk /dev/sdb`

   a. Escriba `d` para eliminar las particiones hasta que no quede ninguna.
   b. Escriba `n` para crear la partición principal 1 que abarca todo el disco.
   c. Escriba `t` para configurar el tipo para una configuración adecuada para el sistema de archivos FAT32, por ejemplo, **c**.
   d. Escriba `p` para imprimir la tabla de particiones.

      El resultado debe ser similar al texto siguiente:

      ```
      Disk /dev/sdb: 2004 MB, 2004877312 bytes
      255 heads, 63 sectors/track, 243 cylinders
      Units = cylinders of 16065 * 512 = 8225280 bytes
         Device Boot      Start         End      Blocks   Id  System
      /dev/sdb1             1           243      1951866  c   W95 FAT32 (LBA)
      ```

   e. Escriba `w` para escribir la tabla de particiones y salir.
3. Formatee la unidad flash USB con el sistema de archivos FAT32.

   `/sbin/mkfs.vfat -F 32 -n USB /dev/sdb1`

4 Cree un directorio de destino y monte la unidad flash USB allí.

```
mkdir -p /usbdisk
mount /dev/sdb1 /usbdisk
```

5 Copie el script de instalación de ESXi en la unidad flash USB.

```
cp ks.cfg /usbdisk
```

6 Desmonte la unidad flash USB.

```
umount /usbdisk
```

Resultados

La unidad flash USB contiene el script de instalación o actualización de ESXi.

Pasos siguientes

Al arrancar el instalador de ESXi, apunte a la ubicación de la unidad flash USB del script de instalación o actualización. Consulte Introducir las opciones de arranque para iniciar un script de instalación o actualización y Archivos de configuración PXELINUX.

Crear una imagen ISO de instalador con un script de instalación o actualización personalizado

Puede personalizar la imagen ISO del instalador de ESXi estándar con su propio script de instalación o actualización. Esta personalización permite realizar una instalación o actualización desatendida y generada por script cuando arranque la imagen ISO del instalador resultante.

Consulte también Acerca de los scripts de instalación y actualización y Acerca del archivo boot.cfg .

Requisitos previos

- Equipo Linux
- La imagen ISO de ESXi `VMware-VMvisor-Installer-6.x.x-XXXXXX.x86_64.iso`, donde `6.x.x` es la versión de ESXi que está instalando y `XXXXXX` es el número de compilación de la imagen ISO del instalador
- Su script de instalación o actualización personalizado, el archivo de inicio `ks_cust.cfg`

Procedimiento

1 Descargue la imagen ISO de ESXi desde el sitio web de VMware.

2 Monte la imagen ISO en una carpeta:

```
mount -o loop VMware-VMvisor-Installer-6.x.x-XXXXXX.x86_64.iso /
esxi_cdrom_mount
```

XXXXXX es el número de versión de ESXi para la versión que está instalado o la versión a la que está actualizando.

3 Copie el contenido de `esxi_cdrom` en otra carpeta:

cp -r /esxi_cdrom_mount/* /esxi_cdrom

4 Copie el archivo de inicio a `/esxi_cdrom`.

cp ks_cust.cfg /esxi_cdrom

5 (opcional) Modifique el archivo `boot.cfg` para especificar la ubicación del script de instalación o actualización a través de la opción `kernelopt`.

Debe utilizar caracteres en mayúscula para proporcionar la ruta de acceso del script, por ejemplo,

```
kernelopt=runweasel ks=cdrom:/KS_CUST.CFG
```

Para el arranque UEFI, debe modificar el archivo `boot.cfg` en `/efi/boot/`.

Este paso automatiza la instalación o la actualización, sin la necesidad de especificar el archivo de inicio durante este proceso.

6 Vuelva a crear la imagen ISO con el comando `mkisofs` o `genisoimage`.

Comando	Sintaxis
mkisofs	**mkisofs -relaxed-filenames -J -R -o custom_esxi.iso -b isolinux.bin -c boot.cat -no-emul-boot -boot-load-size 4 -boot-info-table -eltorito-alt-boot -eltorito-platform efi -b efiboot.img -no-emul-boot /esxi_cdrom**
genisoimage	**genisoimage -relaxed-filenames -J -R -o custom_esxi.iso -b isolinux.bin -c boot.cat -no-emul-boot -boot-load-size 4 -boot-info-table -eltorito-alt-boot -e efiboot.img -no-emul-boot /esxi_cdrom**

Esta imagen ISO se puede utilizar para un arranque normal o el arranque seguro UEFI.

Resultados

La imagen ISO incluye su script de instalación o actualización personalizado.

Pasos siguientes

Instale ESXi desde la imagen ISO.

Arranque PXE del instalador de ESXi

Es posible usar el entorno de ejecución previo al inicio (PXE) para arrancar un host. A partir de vSphere 6.0, es posible arrancar con PXE el instalador de ESXi desde una interfaz de red en los hosts con BIOS heredado o mediante UEFI.

ESXi se distribuye en un formato ISO que está diseñado para instalarse en la memoria flash o en un disco duro local. Puede extraer los archivos y arrancar con PXE.

PXE utiliza el protocolo de configuración dinámica de host (DHCP) y el protocolo trivial de transferencia de archivos (TFTP) para arrancar un sistema operativo a través de una red.

El arranque con PXE requiere determinada infraestructura de red y una máquina con un adaptador de red compatible con PXE. La mayoría de las máquinas que pueden ejecutar ESXi poseen adaptadores de red que pueden arrancar con PXE.

Nota El arranque PXE con firmware de BIOS heredado solo se puede realizar mediante IPv4. El arranque PXE con firmware UEFI se puede realizar mediante IPv4 o IPv6.

Configuraciones de DHCP de muestra

Para el arranque PXE del instalador de ESXi, el servidor DHCP debe enviar la dirección del servidor TFTP y el nombre de archivo del cargador de arranque inicial al host ESXi.

Cuando la máquina de destino arranca por primera vez, transmite un paquete mediante la red para solicitar información a fin de realizar el arranque por sí misma. El servidor DHCP responde. El servidor DHCP debe ser capaz de determinar si la máquina de destino puede arrancar y, asimismo, de determinar la ubicación del archivo binario del cargador de arranque inicial (generalmente un archivo en un servidor TFTP).

Precaución No configure un segundo servidor DHCP si la red ya tiene uno. Si varios servidores DHCP responden a las solicitudes de DHCP, las máquinas pueden obtener direcciones IP incorrectas o en conflicto, o no recibir la información de arranque correcta. Consulte a un administrador de red antes de configurar un servidor DHCP. Para obtener asistencia en relación con la configuración de DHCP, póngase en contacto con el proveedor del servidor DHCP.

Muchos servidores DHCP tienen hosts de arranque mediante PXE. Si usa una versión de DHCP para Microsoft Windows, consulte la documentación del servidor DHCP para determinar cómo transmitir los argumentos `next-server` y `filename` a la máquina de destino.

Ejemplo de arranque mediante TFTP con IPv4

En este ejemplo se muestra cómo configurar un servidor DHCP de ISC para arrancar ESXi mediante un servidor TFTP en una dirección IPv4 xxx.xxx.xxx.xxx.

```
#
# ISC DHCP server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;
option client-system-arch code 93 = unsigned integer 16;
class "pxeclients" {
   match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
   next-server xxx.xxx.xxx.xxx;
   if option client-system-arch = 00:07 or option client-system-arch = 00:09 {
      filename = "mboot.efi";
   } else {
      filename = "pxelinux.0";
   }
}
```

Cuando una máquina intenta realizar un arranque PXE, el servidor DHCP proporciona una dirección IP y la ubicación del archivo binario `pxelinux.0` o `mboot.efi` en el servidor TFTP.

Ejemplo de arranque mediante TFTP con IPv6

En este ejemplo se muestra cómo configurar un servidor DHCPv6 de ISC para arrancar ESXi mediante un servidor TFTP en una dirección IPv6 xxxx:xxxx:xxxx:xxxx::xxxx.

```
#
# ISC DHCPv6 server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;
option dhcp6.bootfile-url code 59 = string;
option dhcp6.bootfile-url "tftp://[xxxx:xxxx:xxxx:xxxx::xxxx]/mboot.efi";
```

Cuando una máquina intenta realizar un arranque PXE, el servidor DHCP proporciona una dirección IP y la ubicación del archivo binario `mboot.efi` en el servidor TFTP.

Ejemplo de arranque mediante HTTP con IPv4

En este ejemplo se muestra cómo configurar un servidor DHCP de ISC para arrancar ESXi mediante un servidor web en una dirección IPv4 xxx.xxx.xxx.xxx. El ejemplo utiliza gPXELINUX para los hosts de BIOS heredado e iPXE para los hosts UEFI.

```
#
# ISC DHCPv6 server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;
option client-system-arch code 93 = unsigned integer 16;
class "pxeclients" {
   match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
   next-server xxx.xxx.xxx.xxx;
   if option client-system-arch = 00:07 or option client-system-arch = 00:09 {
      if exists user-class and option user-class = "iPXE" {
         # Instruct iPXE to load mboot.efi as secondary bootloader
         filename = "mboot.efi";
      } else {
         # Load the snponly.efi configuration of iPXE as initial bootloader
         filename = "snponly.efi";
      }
   } else {
      filename "gpxelinux.0";
   }
}
```

Cuando una máquina intenta realizar un arranque PXE, el servidor DHCP proporciona una dirección IP y la ubicación del archivo binario `gpxelinux.0` o `snponly.efi` en el servidor TFTP. En el caso de UEFI, iPXE pide al servidor DHCP el siguiente archivo que se debe cargar y, en esta ocasión, el servidor devuelve el nombre de archivo `mboot.efi`.

Ejemplo de arranque mediante HTTP con IPv6

En este ejemplo se muestra cómo configurar un servidor DHCPv6 de ISC para arrancar ESXi mediante un servidor TFTP en una dirección IPv6 xxxx:xxxx:xxxx:xxxx::xxxx.

```
#
# ISC DHCPv6 server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;

option dhcp6.bootfile-url code 59 = string;
if exists user-class and option user-class = "iPXE" {
   # Instruct iPXE to load mboot.efi as secondary bootloader
   option dhcp6.bootfile-url "tftp://[xxxx:xxxx:xxxx:xxxx::xxxx]/mboot.efi";
} else {
   # Load the snponly.efi configuration of iPXE as initial bootloader
   option dhcp6.bootfile-url "tftp://[xxxx:xxxx:xxxx:xxxx::xxxx]/snponly.efi";
}
```

Cuando una máquina intenta realizar un arranque PXE, el servidor DHCP proporciona una dirección IP y la ubicación del archivo binario `snponly.efi` (iPXE) en el servidor TFTP. iPXE pide al servidor DHCP el siguiente archivo que se debe cargar y, en esta ocasión, el servidor devuelve el nombre de archivo `mboot.efi`.

Archivos de configuración PXELINUX

Se necesita un archivo de configuración PXELINUX para iniciar el instalador de ESXi en un sistema BIOS heredado. El archivo de configuración define el menú que se debe mostrar en el host ESXi de destino mientras se inicia y se pone en contacto con el servidor TFTP para obtener toda la configuración de SYSLINUX, incluidos los valores de PXELINUX y gPXELINUX.

En esta sección, se brinda información general sobre los archivos de configuración PXELINUX. Para ver ejemplos, consulte Configuraciones de DHCP de muestra.

Para conocer detalles de la sintaxis, visite el sitio web de SYSLINUX en http://www.syslinux.org/.

Archivos requeridos

En el archivo de configuración de PXE, debe incluir rutas de acceso a los siguientes archivos:

- `mboot.c32` es el cargador de arranque.
- `boot.cfg` es el archivo de configuración del cargador de arranque.

Consulte Acerca del archivo boot.cfg

Nombre del archivo de configuración de PXE

Para el nombre del archivo de configuración de PXE, seleccione una de las siguientes opciones:

- `01-`*`mac_address_of_target_ESXi_host`*. Por ejemplo, `01-23-45-67-89-0a-bc`
- La dirección IP del host ESXi de destino en anotación hexadecimal.
- `default`

El archivo de arranque inicial, `pxelinux.0` o `gpxelinux.0`, intenta cargar un archivo de configuración de PXE en el siguiente orden:

1. Intenta con la dirección MAC del host ESXi de destino, con su código de tipo ARP, que es 01 para Ethernet, como prefijo.
2. Si ese intento genera un error, intenta con la anotación hexadecimal de la dirección IP del sistema ESXi de destino.
3. Por último, intenta cargar un archivo con el nombre `default`.

Ubicación del archivo de configuración de PXE

Guarde el archivo en `/tftpboot/pxelinux.cfg/` en el servidor TFTP.

Por ejemplo, es posible guardar el archivo en el servidor TFTP en `/tftpboot/pxelinux.cfg/01-00-21-5a-ce-40-f6`. La dirección MAC del adaptador de red del host ESXi de destino es 00-21-5a-ce-40-f6.

Información sobre el arranque PXE

Comprender el proceso de arranque PXE puede ayudarle durante la solución de problemas.

Servidor TFTP

El protocolo trivial de transferencia de archivos (TFTP) es similar al servicio FTP y se utiliza generalmente solo para los sistemas de arranque de red o la carga de firmware en dispositivos de red, como los enrutadores. TFTP está disponible en Linux y Windows.

- La mayoría de las distribuciones de Linux incluyen una copia del servidor tftp-hpa. Si requiere una solución compatible, adquiera un servidor TFTP compatible de su proveedor de confianza. También puede adquirir un servidor TFTP desde uno de los dispositivos de paquete en VMware Marketplace.
- Si su servidor TFTP va a funcionar en un host de Microsoft Windows, utilice tftpd32 versión 2.11 o posterior. Consulte http://tftpd32.jounin.net/.

SYSLINUX, PXELINUX y gPXELINUX

Si utiliza PXE en un entorno BIOS heredado, debe tener conocimientos acerca de los distintos entornos de arranque.

- SYSLINUX es un entorno de arranque de código abierto para máquinas que ejecutan firmware de BIOS heredado. El cargador de arranque de ESXi para sistemas BIOS, `mbootc.32`, se ejecuta como un complemento de SYSLINUX. Puede configurar SYSLINUX para el arranque desde distintos tipos de medios, como un disco, una imagen ISO y una red. Puede encontrar el paquete de SYSLINUX en http://www.kernel.org/pub/linux/utils/boot/syslinux/.
- PXELINUX es una configuración de SYSXLINUX para realizar el arranque desde un servidor TFTP, según el estándar PXE. Si utiliza PXELINUX para arrancar el instalador de ESXi, el archivo binario `pxelinux.0`, `mboot.c32`, el archivo de configuración, el kernel y otros archivos se transfieren mediante TFTP.
- gPXELINUX es una configuración híbrida que incluye tanto PXELINUX como gPXE y admite el arranque desde un servidor web. gPXELINUX es parte de un paquete de SYSLINUX. Si utiliza gPXELINUX para arrancar el instalador de ESXi, solo el archivo binario `gpxelinux.0`, `mboot.c32` y el archivo de configuración se transfieren mediante TFTP. El resto de los archivos se transfiere mediante HTTP. HTTP suele ser más rápido y fiable que TFTP, especialmente en lo que respecta a la transferencia de grandes cantidades de datos en redes muy cargadas.

Nota Actualmente, VMware compila el complemento `mboot.c32` para que funcione con la versión 3.86 de SYSLINUX y prueba el arranque PXE solo con esa versión. Puede que otras versiones no sean compatibles. Esta no es una declaración de compatibilidad limitada. En el caso de la compatibilidad de agentes de terceros que utilice para configurar su infraestructura de arranque PXE, póngase en contacto con el proveedor.

---

iPXE y PXE de UEFI

La mayoría del firmware UEFI es compatible de forma nativa con PXE, lo que permite arrancar desde un servidor TFTP. El firmware puede cargar directamente el cargador de arranque de ESXi para los sistemas UEFI, `mboot.efi`. No es necesario ningún software adicional (p. ej., PXELINUX).

iPXE también puede ser útil para sistemas UEFI que no incluyan PXE en el firmware y para sistemas UEFI más antiguos con errores en la compatibilidad con PXE. En estos casos, puede intentar instalar iPXE en una unidad flash USB y arrancar desde ahí.

Nota Los productos Apple Macintosh no son compatibles con el arranque PXE. En su lugar, son compatibles con el arranque de red mediante un protocolo específico para Apple.

Métodos alternativos para el arranque PXE

También existen métodos alternativos para el arranque PXE de software y hosts distintos, por ejemplo:

- Configuración del servidor DHCP para que proporcione diferentes nombres de archivo del cargador de arranque inicial a distintos hosts según la dirección MAC u otros criterios. Consulte la documentación del servidor DCHP.
- Métodos que utilizan iPXE como cargador de arranque inicial con un archivo de configuración de iPXE que selecciona el siguiente cargador de arranque según la dirección MAC u otros criterios.

Instalar y arrancar ESXi con FCoE de software

Puede instalar y arrancar ESXi desde un LUN FCoE utilizando los adaptadores FCoE de software VMware y los adaptadores de red con capacidades de descarga FCoE. Su host no requiere un HBA FCoE dedicado.

Consulte la documentación de *Almacenamiento de vSphere* para obtener información sobre la instalación y el arranque de ESXi con FCoE para software.

Usar aplicaciones de administración remota

Las aplicaciones de administración remota permiten instalar ESXi en servidores que se encuentran en ubicaciones remotas.

Las aplicaciones de administración remota compatibles para la instalación incluyen HP Integrated Lights-Out (iLO), Dell Remote Access Card (DRAC), IBM management module (MM) y Remote Supervisor Adapter II (RSA II). Para obtener una lista de modelos de servidores compatibles y versiones de firmware de administración remota, consulte Modelos de servidores de administración remota compatibles y versiones de firmware. Para obtener soporte técnico para las aplicaciones de administración remota, póngase en contacto con el proveedor.

Puede usar aplicaciones de administración remota para realizar instalaciones interactivas y por script de ESXi de forma remota.

Si utiliza aplicaciones de administración remota para instalar ESXi, el CD virtual podría encontrarse con daños en sistemas o redes que operan a capacidad máxima. Si se produce un error en una instalación remota de una imagen ISO, complete la instalación desde el CD físico.

Personalizar instalaciones con vSphere ESXi Image Builder

Se puede usar VMware vSphere® ESXi™ Image Builder CLI para crear imágenes de instalación de ESXi con un conjunto personalizado de actualizaciones, revisiones y controladores.

Se puede usar vSphere ESXi Image Builder con vSphere Web Client o con PowerCLI para crear una imagen de instalación de ESXi con un conjunto personalizado de actualizaciones y revisiones de ESXi. También se pueden incluir controladores de almacenamiento o red de otros fabricantes que se lancen entre versiones de vSphere.

Se puede implementar una imagen de ESXi creada con vSphere ESXi Image Builder de cualquiera de las siguientes maneras:

- Grabando la imagen en un DVD de instalación.
- Mediante vCenter Server, utilizando la característica Auto Deploy.

Información sobre vSphere ESXi Image Builder

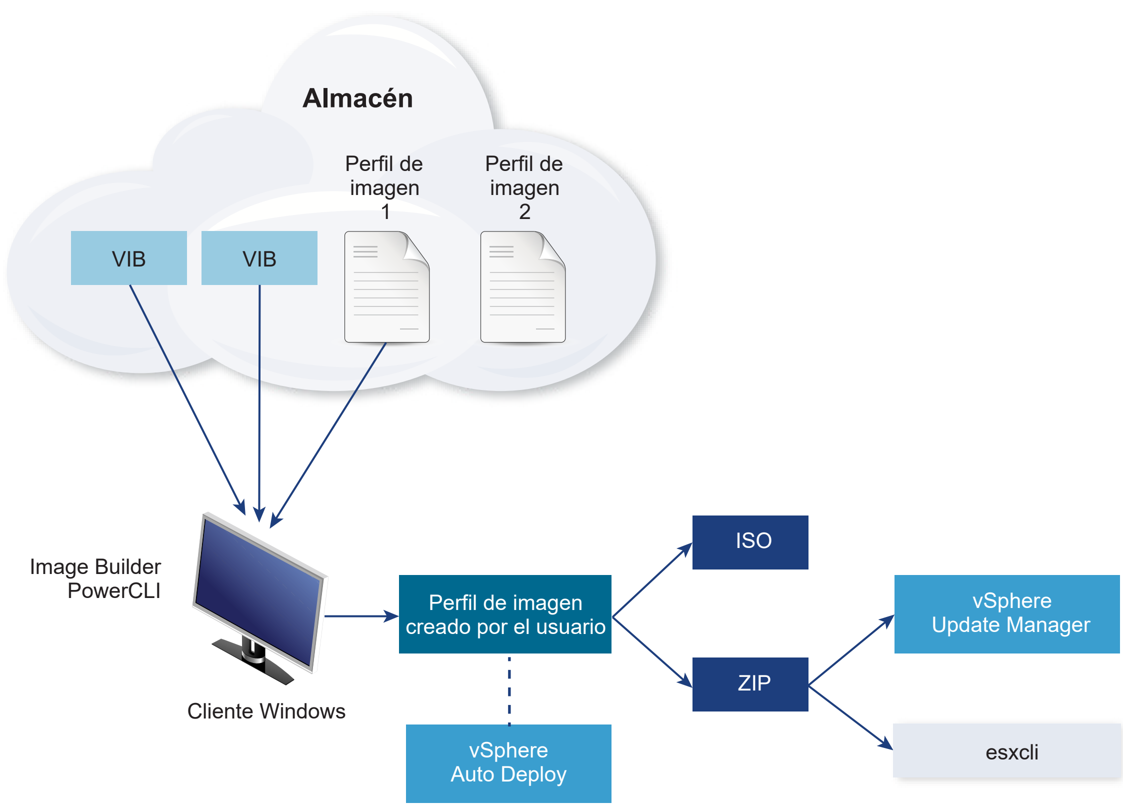
Puede utilizar VMware vSphere® ESXi™ Image Builder CLI para administrar almacenes de software, perfiles de imagen y paquetes de software (VIB). Los perfiles de imagen y los VIB especifican el software que desea utilizar durante la instalación o actualización de un host ESXi.

Descripción general de vSphere ESXi Image Builder

vSphere ESXi Image Builder permite administrar perfiles de imágenes y VIB de vSphere.

Los VIB son paquetes de software; los perfiles de imágenes contienen un conjunto de paquetes de software. Consulte Almacenes de software y sus componentes.

Figura 2-2. Arquitectura de Image Builder



Puede usar cmdlets de vSphere ESXi Image Builder a fin de administrar el software para implementar en los hosts ESXi en varias situaciones diferentes.

Tabla 2-7. Casos en los que se puede utilizar vSphere ESXi Image Builder

Caso de uso para vSphere ESXi Image Builder	Descripción
Crear perfiles de imágenes para que use vSphere Auto Deploy	Use vSphere ESXi Image Builder para crear un perfil de imagen que defina los VIB que vSphere Auto Deploy emplea para aprovisionar hosts.
Agregar controladores de terceros personalizados a un perfil de imagen existente y exportarlos a un ISO o paquete	Cuando agregue un controlador de terceros o VIB personalizados de extensión a sus hosts ESXi, use vSphere ESXi Image Builder para clonar la imagen base que proporcione VMware, agregue los VIB personalizados y expórtelos a un archivo ISO o un archivo ZIP en paquete sin conexión.
Realización de actualizaciones	Si actualiza desde un sistema 4.0 o 4.1 que incluye extensiones o controladores personalizados, puede usar vSphere ESXi Image Builder para crear un perfil de imagen que incluya el VIB base de vSphere 5. Puede crear VIB de vSphere 5 para las extensiones personalizadas y agregar dichos VIB al VIB base. Exporte el perfil de imagen personalizado a un archivo ISO que puede instalar o un archivo ZIP que puede usar con vSphere Update Manager.
Creación de imágenes personalizadas con tamaño reducido	Si requiere una imagen de tamaño mínimo, puede clonar el perfil de imagen base de ESXi y quitar VIB mediante vSphere ESXi Image Builder.

Los cmdlets de vSphere ESXi Image Builder toman perfiles de imágenes y VIB como archivo de entrada y producen diversos archivos de salida.

Tabla 2-8. Archivos de entrada y salida de los cmdlets de vSphere ESXi Image Builder

Parámetro	Descripción
Archivo de entrada	Los perfiles de imágenes y los VIB se encuentran ubicados en un almacén de software y se usan como archivos de entrada para cmdlets de PowerCLI que se ejecutan en un cliente de Windows.
Archivos de salida	Los cmdlets de PowerCLI crean perfiles de imágenes personalizados que se pueden exportar a un archivo de imagen ISO o un archivo ZIP de almacén sin conexión. Para la instalación se usan imágenes ISO. El almacén de ZIP puede usarse mediante Update Manager o a través de comandos `esxcli software` para actualizar o instalar imágenes. Los perfiles de imágenes también se usan en reglas de vSphere Auto Deploy para personalizar el software con que se aprovisionan los hosts ESXi.

Vea el vídeo Uso de Image Builder CLI para obtener información sobre vSphere ESXi Image Builder:

Using Image Builder CLI
(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_vvb0gt3i/uiConfId/49694343/)

Almacenes de software y sus componentes

Comprender cómo están estructurados los almacenes, perfiles y VIB y dónde puede utilizarlos es un requisito previo para la instalación en la memoria de una imagen ISO personalizada de ESXi, para el aprovisionamiento de hosts ESXi con vSphere Auto Deploy y para determinadas operaciones de actualización personalizadas.

Los siguientes términos técnicos se utilizan en toda la documentación de vSphere en asuntos relacionados con tareas de instalación y actualización.

VIB

Un VIB es un paquete de software de ESXi. VMware y sus soluciones de paquetes de partners, controladores, proveedores de CIM y aplicaciones que extienden la plataforma de ESXi como VIB. Los VIB están disponibles en almacenes de software. Puede usar VIB para crear y personalizar imágenes ISO o para actualizar hosts ESXi mediante la instalación de VIB de forma asincrónica en los hosts.

Consulte Propiedades del objeto SoftwarePackage.

Perfil de imagen

Un perfil de imagen define una imagen de ESXi y consta de VIB. Un perfil de imagen incluye un VIB base y también podría incluir más VIB. Es posible analizar y definir un perfil de imagen mediante vSphere ESXi Image Builder.

Consulte Propiedades del objeto ImageProfile.

Almacén de software

Un almacén de software es una colección de VIB y perfiles de imagen. El almacén de software es una jerarquía de archivos y carpetas, y puede estar disponible a través de una URL HTTP (almacén en línea) o un archivo ZIP (almacén sin conexión). Los partners VMware y VMware se encargan de que los almacenes estén disponibles. Las compañías con instalaciones de VMware grandes podrían crear almacenes internos para aprovisionar hosts ESXi con vSphere Auto Deploy o para exportar un imagen ISO para la instalación de ESXi.

Descripción general de cmdlets de vSphere ESXi Image Builder

Los cmdlets de vSphere ESXi Image Builder permiten administrar perfiles de imagen y VIB.

vSphere ESXi Image Builder incluye los siguientes cmdlets.

Nota Durante la ejecución de cmdlets de vSphere ESXi Image Builder, al invocar el cmdlet, proporcione todos los parámetros en la línea de comandos. No se recomienda proporcionar parámetros en modo interactivo.

Ejecute `Get-Help` *cmdlet_name* en el símbolo de PowerCLI para obtener información de referencia detallada.

Tabla 2-9. Cmdlets de vSphere ESXi Image Builder

Cmdlet	Descripción
`Add-EsxSoftwareDepot`	Agregar el almacén de software o el archivo ZIP en la ubicación especificada del entorno actual. Descarga metadatos del almacén y analiza los VIB para comprobar si tienen dependencias.
`Remove-EsxSoftwareDepot`	Se desconecta del almacén de software especificado.
`Get-EsxSoftwareDepot`	Devuelve una lista de almacenes de software que se encuentran en el entorno actual. Si desea examinar y administrar perfiles de imagen y VIB, primero debe agregar el almacén de software correspondiente al entorno.
`Get-EsxSoftwarePackage`	Devuelve una lista de objetos de paquete de software (VIB). Utilice estas opciones del cmdlet para filtrar los resultados.
`Get-EsxImageProfile`	Devuelve una matriz de objetos `ImageProfile` de todos los almacenes agregados actualmente.
`New-EsxImageProfile`	Crea un nuevo perfil de imagen. En la mayoría de los casos, se recomienda crear un nuevo perfil mediante la clonación de un perfil existente. Consulte Clonar un perfil de imagen.
`Set-EsxImageProfile`	Modifica un objeto `ImageProfile` local y realiza pruebas de validación en el perfil modificado. El cmdlet devuelve el objeto modificado pero no lo conserva.
`Export-EsxImageProfile`	Exporta un perfil de imagen como una imagen ISO de ESXi para instalar ESXi, o bien como un archivo ZIP.
`Compare-EsxImageProfile`	Devuelve una estructura `ImageProfileDiff` que muestra si dos perfiles tienen la misma lista de VIB y el mismo nivel de aceptación. Consulte Niveles de aceptación.
`Remove-EsxImageProfile`	Elimina el perfil de imagen del almacén de software.
`Add-EsxSoftwarePackage`	Agrega uno o más paquetes (VIB) nuevos a un perfil de imagen existente.
`Remove-EsxSoftwarePackage`	Elimina uno o más paquetes (VIB) de un perfil de imagen.

Perfiles de imagen

Los perfiles de imagen definen el conjunto de VIB que utiliza un proceso de instalación o actualización de ESXi. Los perfiles de imagen se aplican a hosts aprovisionados con vSphere Auto Deploy y a otros hosts ESXi 5.x. El usuario define y manipula los perfiles de imagen con vSphere ESXi Image Builder.

Requisitos de los perfiles de imagen

Puede crear un perfil de imagen personalizado desde cero o clonar uno existente y agregarle o quitarle VIB. Para que sean válidos, los perfiles deben cumplir los siguientes requisitos.

- Cada perfil de imagen debe tener una combinación de nombre y proveedor única.
- Además, cada uno tiene un nivel de aceptación. Cuando agrega un VIB a un perfil de imagen con un cmdlet de vSphere ESXi Image Builder, este programa comprueba que el VIB coincida con el nivel de aceptación definido para el perfil.

- No puede quitar VIB que son necesarios para otros VIB.
- Tampoco puede incluir dos versiones del mismo VIB en un perfil de imagen. Cuando se agrega una nueva versión de un VIB, esta reemplaza a la versión existente.

Validar un perfil de imagen

Para que sean válidos, los perfiles de imagen y sus VIB deben cumplir varios criterios.

- Los perfiles de imagen deben contener al menos un VIB de base y un módulo de kernel de arranque.
- Si algún VIB del perfil de imagen depende de otro VIB, este otro también tendrá que estar incluido en el perfil de imagen. Los creadores de VIB almacenan esa información en la propiedad Depends del objeto SoftwarePackage.
- Los VIB no deben entrar en conflicto entre sí. Los creadores de VIB almacenan la información sobre conflictos en la propiedad Conflicts del objeto SoftwarePackage.
- Dos VIB con el mismo nombre, pero de dos versiones diferentes, no pueden coexistir. Cuando se agrega una nueva versión de un VIB, esta reemplaza a la versión existente.
- Hay problemas de falta de validación del nivel de aceptación.

Cuando se realiza un cambio en un perfil de imagen, vSphere ESXi Image Builder comprueba que el cambio no invalide el perfil.

Validación de dependencias

Cuando se agrega o se quita un VIB, vSphere ESXi Image Builder comprueba que se cumplan las dependencias del paquete. Cada objeto SoftwarePackage incluye una propiedad Depends que especifica una lista de otros VIB de los que depende ese VIB. Consulte Estructura de los objetos ImageProfile, SoftwarePackage e ImageProfileDiff

Validación del nivel de aceptación

vSphere ESXi Image Builder realiza una validación del nivel de aceptación cada vez que se crea o se modifica un perfil de imagen. vSphere ESXi Image Builder comprueba el nivel de aceptación de los VIB del perfil de imagen con el nivel de aceptación mínimo permitido del perfil. El nivel de aceptación del VIB también se valida cada vez que se valida la firma de un VIB.

Validar VIB durante la exportación

Cuando se exporta un perfil de imagen a una imagen ISO, vSphere ESXi Image Builder valida todos los VIB mediante las siguientes acciones.

- Comprueba que no haya conflictos mediante la comprobación de la propiedad Conflicts de todos los objetos SoftwarePackage.

- Realiza una validación de firma de VIB. La validación de la firma evita que se realicen modificaciones no autorizadas a los paquetes de VIB. La firma es una suma de comprobación criptográfica que garantiza que un determinado autor produjo el VIB. La validación de la firma también se lleva a cabo durante la instalación de VIB en un host ESXi y cuando el servidor vSphere Auto Deploy utiliza VIB.
- Comprueba que los VIB respeten las reglas de uso de rutas de archivo. VMware prueba los VIB VMwareCertified y VMwareAccepted para garantizar que estos respeten siempre las reglas de uso de rutas de archivo.

Niveles de aceptación

Cada VIB se lanza con un nivel de aceptación que no se puede cambiar. El nivel de aceptación del host determina qué VIB pueden instalarse en un host. Puede cambiar los niveles de aceptación del host mediante los comandos de `esxcli`.

VMware admite los siguientes niveles de aceptación.

VMwareCertified

El nivel de aceptación VMwareCertified tiene los requisitos más estrictos. Los VIB con este nivel se someten a pruebas completamente equivalentes a las pruebas de control de calidad internas de VMware para la misma tecnología. Hoy en día, solo los controladores de los programas de proveedores de E/S (I/O Vendor Program, IOVP) se publican en este nivel. VMware responde a las llamadas de soporte para VIB con este nivel de aceptación.

VMwareAccepted

Los VIB con este nivel de aceptación pasan por pruebas de comprobación, pero estas no prueban completamente todas las funciones del software. El partner realiza pruebas y VMware comprueba el resultado. Hoy en día, los proveedores de CIM y los complementos de PSA son algunos de los VIB que se publican en este nivel. VMware dirige las llamadas de soporte para VIB con este nivel de aceptación a la organización de soporte del partner.

PartnerSupported

Los VIB con el nivel de aceptación PartnerSupported los publica un partner de confianza de VMware. El partner realiza todas las pruebas. VMware no comprueba los resultados. Este nivel se utiliza para una tecnología nueva o alternativa que los partners desean habilitar para los sistemas VMware. Hoy en día, las tecnologías de VIB de controlador, como Infiniband, ATAoE y SSD, se encuentran en este nivel con controladores de hardware que no son estándar. VMware dirige las llamadas de soporte para VIB con este nivel de aceptación a la organización de soporte del partner.

CommunitySupported

El nivel de aceptación CommunitySupported es para VIB creados por personas o empresas por fuera de los programas de partners de VMware. Los VIB de este nivel de aceptación no pasaron por un programa de pruebas aprobado por VMware y no son compatibles con el soporte técnico de VMware ni los partners de VMware.

Estructura de los objetos ImageProfile, SoftwarePackage e ImageProfileDiff

Conocer la estructura de los objetos `ImageProfile`, `SoftwarePackage` y `ImageProfileDiff` ayuda a administrar los procesos de implementación y actualización.

Propiedades del objeto ImageProfile

El objeto `ImageProfile`, al que se puede acceder con el cmdlet de `Get-EsxImageProfile`PowerCLI, posee las siguientes propiedades.

Nombre	Tipo	Descripción
`AcceptanceLevel`	`AcceptanceLevel`	Determina qué VIB se pueden agregar al perfil. Los niveles son VMwareCertified, VMwareAccepted, PartnerSupported y CommunitySupported. Consulte Niveles de aceptación.
`Author`	`System.String`	La persona que creó el perfil. 60 caracteres o menos.
`CreationTime`	`System.DateTime`	Marca de hora de creación.
`Description`	`System.String`	La descripción de texto completo del perfil. Sin límite de longitud.
`GUID`	`System.String`	Identificador único global del perfil de imagen.
`ModifiedTime`	`System.DateTime`	Marca de hora de la última modificación.
`Name`	`System.String`	Nombre del perfil de imagen. 80 caracteres o menos.
`ReadOnly`	`System.Boolean`	Cuando se establece en `true`, el perfil no se puede editar. Utilice `Set-EsxImageProfile -Readonly` para lograr que los perfiles de imagen personalizados sean de solo lectura.
`Rules`	`ImageProfileRule[]`	Cualquier restricción o requisito de hardware OEM que el perfil de imagen podría tener. vSphere Auto Deploy verifica el valor de esta propiedad al implementar un perfil de imagen, e implementa el perfil si se encuentra disponible hardware coincidente.
`Vendor`	`System.String`	La organización que publica el perfil. 40 caracteres o menos.
`VibList`	`SoftwarePackage[]`	La lista de identificadores de VIB que la imagen contiene.

Propiedades del objeto SoftwarePackage

Al preparar un perfil de imagen, puede examinar los paquetes de software para decidir qué paquetes son adecuados para la inclusión. El objeto `SoftwarePackage` posee las siguientes propiedades.

Nombre	Tipo	Descripción
`AcceptanceLevel`	`AcceptanceLevel`	El nivel de aceptación de este VIB.
`Conflicts`	`SoftwareConstraint[]`	Una lista de VIB que no se pueden instalar al mismo tiempo que este VIB. Cada limitación utiliza el siguiente formato: `package-name[<<|<=|=|>=|<< version]`
`Depends`	`SoftwareConstraint[]`	Una lista de VIB que deben instalarse al mismo tiempo que este VIB. Mismo formato de limitación que la propiedad `Conflicts`.
`Description`	`System.String`	La descripción extensa de VIB.
`Guid`	`System.String`	El identificador único del VIB.
`LiveInstallOk`	`System.Boolean`	Valor “True” si se admiten las instalaciones activas en este VIB.
`LiveRemoveOk`	`System.Boolean`	Valor “True” si se admiten las eliminaciones activas en este VIB.
`MaintenanceMode`	`System.Boolean`	Valor “True” si los hosts deben estar en el modo de mantenimiento para la instalación de este VIB.
`Name`	`System.String`	Nombre del VIB. Generalmente describe de forma exclusiva al paquete en un sistema ESXi en ejecución.
`Provides`	`SoftwareProvides`	La lista de paquetes virtuales o interferencias que este VIB proporciona. Consulte Propiedades del objeto SoftwareProvide.
`ReferenceURLs`	`SupportReference[]`	La lista de objetos `SupportReference` con información de apoyo exhaustiva. El objeto `SupportReference` posee dos propiedades,`Title` y `URL`, ambas del tipo `System.String`.
`Replaces`	`SoftwareConstraint[]`	La lista de objetos `SoftwareConstraint` que identifica a los VIB que reemplazan a este VIB o lo vuelven obsoleto. Los VIB reemplazan automáticamente a los VIB con el mismo nombre, pero de versiones anteriores.

Nombre	Tipo	Descripción
`ReleaseDate`	`System.DateTime`	Fecha y hora de publicación o lanzamiento del VIB.
`SourceUrls`	`System.String[]`	La lista de URL de origen desde la que se puede descargar este VIB.
`StatelessReady`	`System.Boolean`	Valor "True" si el paquete es compatible con perfiles de host u otras tecnologías que permiten que sea adecuado para la utilización en conjunto con vSphere Auto Deploy.
`Summary`	`System.String`	Resumen de una línea del VIB.
`Tags`	`System.String[]`	Matriz de etiquetas de cadenas para este paquete definido por el proveedor o editor. Las etiquetas pueden utilizarse para identificar características del paquete.
`Vendor`	`System.String`	Proveedor o editor del VIB.
`Version`	`System.String`	Versión del VIB.
`VersionObject`	`Software.Version`	La propiedad `VersionObject` es del tipo `SoftwareVersion`. La clase `SoftwareVersion` implementa un método `Compare` estático para comparar dos versiones de cadenas. Consulte Propiedades del objeto SoftwareVersion

Propiedades del objeto ImageProfileDiff

Cuando ejecute el cmdlet `Compare-EsxImageProfile`, puede transferir dos parámetros, primero el perfil de referencia y, a continuación, el perfil de comparación. El cmdlet devuelve un objeto `ImageProfileDiff`, que posee las siguientes propiedades.

Nombre	Tipo	Descripción
`CompAcceptanceLevel`	`System.String`	El nivel de aceptación para el segundo perfil que se transfirió a `Compare-EsxImageProfile`.
`DowngradeFromRef`	`System.String[]`	La lista de VIB en el segundo perfil que son degradaciones de los VIB del primer perfil.
`Equal`	`System.Boolean`	Valor `True` si los dos perfiles de imagen poseen paquetes y niveles de aceptación idénticos.
`OnlyInComp`	`System.String`	La lista de VIB encontrados solo en el segundo perfil que se transfirió a `Compare-EsxImageProfile`.

Nombre	Tipo	Descripción
`OnlyInRef`	`System.String[]`	La lista de VIB encontrados solo en el primer perfil que se transfirió a `Compare-EsxImageProfile`.
`PackagesEqual`	`System.Boolean`	`True` si los perfiles de imagen poseen conjuntos idénticos de paquetes de VIB.
`RefAcceptanceLevel`	`System.String`	El nivel de aceptación para el primer perfil que se transfirió a `Compare-EsxImageProfile`.
`UpgradeFromRef`	`System.String[]`	La lista de VIB en el segundo perfil que son actualizaciones de los VIB del primer perfil.

Propiedades del objeto SoftwareVersion

El objeto `SoftwareVersion` permite comparar dos cadenas de versión. El objeto incluye un método `Compare` estático que acepta dos cadenas como entrada y devuelve `1` si la primera cadena de versión es un número superior a la segunda cadena de versión. `Compare` devuelve `0` si las dos cadenas de versión son iguales. `Compare`devuelve `-1` si la segunda cadena de versión es un número superior al de la primera cadena. El objeto posee las siguientes propiedades.

Nombre	Tipo	Descripción
`Version`	`System.String`	La parte de la versión antes del guión. Esta parte indica la versión principal.
`Release`	`System.String`	La parte de la versión después del guión. Esta parte indica la versión de la revisión.

Propiedades del objeto SoftwareConstraint

El objeto `SoftwareConstraint` implementa un método `MatchesProvide`. El método acepta un objeto `SoftwareProvides` o `SoftwarePackage` como entrada y devuelve `True` si la limitación coincide con `SoftwareProvide` o `SoftwarePackage` o, de lo contrario, devuelve `False`.

El objeto `SoftwareConstraint` posee las siguientes propiedades.

Nombre	Tipo	Descripción
`Name`	`System.String`	Nombre de la limitación. Este nombre debe coincidir con una propiedad `SoftwareProvideName` correspondiente.
`Relation`	`System.String`	Una enumeración o uno de los siguientes indicadores de comparación: <<, <=, = >=, >>. Esta propiedad puede ser $null si la limitación no posee una propiedad `Relation` y `Version`.

Nombre	Tipo	Descripción
Version	System.String	La versión para hacer coincidir la limitación. Esta propiedad puede ser $null si la limitación no posee una propiedad Relation y Version.
VersionObject	SoftwareVersion	La versión representada por un objeto SoftwareVersion.

Propiedades del objeto SoftwareProvide

El objeto SoftwareProvide posee las siguientes propiedades.

Nombre	Tipo	Descripción
Name	System.String	Nombre del suministro.
Version	System.String	Versión del suministro. Puede ser $null si el suministro no especifica una versión.
Release	System.String	La versión del suministro tal como se representa a través de un objeto SoftwareVersion. Consulte Propiedades del objeto SoftwareVersion.

Instalar y usar vSphere ESXi Image Builder

vSphere ESXi Image Builder está compuesto por el servidor de vSphere ESXi Image Builder y los cmdlets de PowerShell de vSphere ESXi Image Builder. El servidor de vSphere ESXi Image Builder se inicia cuando se ejecuta el primer cmdlet de vSphere ESXi Image Builder.

Instalar vSphere ESXi Image Builder y software de requisito previo

Antes de que pueda ejecutar los cmdlets de vSphere ESXi Image Builder, deberá instalar PowerCLI y todo el software de requisito previo. El complemento vSphere ESXi Image Builder se incluye con la instalación de PowerCLI.

Requisitos previos

Si desea administrar vSphere ESXi Image Builder con cmdlets de PowerCLI, compruebe que Microsoft .NET Framework 4.5 o 4.5.x y Windows PowerShell 3.0 o 4.0 se encuentren instalados en un sistema Microsoft Windows. Consulte la Guía del usuario de PowerCLI.

Procedimiento

1 Abra PowerShell en su estación de trabajo.

2 Descargue una versión de PowerCLI posterior a PowerCLI 6.5R1 de la página de inicio de PowerCLI.

3 Para instalar todos los módulos de PowerCLI, ejecute el comando: `Install-Module VMware.PowerCLI -Scope CurrentUser`. Como alternativa, puede instalar módulos de PowerCLI individuales si ejecuta el cmdlet Install-Module con el nombre del módulo. Si aparece una advertencia de que está instalando módulos de un repositorio que no es de confianza, presione **y** y luego presione **Intro** para confirmar la instalación.

   Puede comprobar que el módulo de PowerCLI esté disponible mediante el comando

   `Get-Module -Name VMware.PowerCLI -ListAvailable`.

Pasos siguientes

Revise Usar los cmdlets de vSphere ESXi Image Builder . Si no está familiarizado con PowerCLI, lea la *Guía del usuario de PowerCLI*.

Utilice los cmdlets de vSphere ESXi Image Builder y otros cmdlets de PowerCLI y cmdlets de PowerShell para administrar los perfiles de imagen y VIB. Utilice `Get-Help` *nombre_del_cmdlet* en cualquier momento para obtener ayuda en la línea de comandos.

Configurar el tipo de inicio del servicio vSphere ESXi Image Builder

Antes de que pueda usar vSphere ESXi Image Builder con vSphere Web Client, debe comprobar que el servicio esté habilitado y en ejecución.

Procedimiento

1 Inicie sesión en el sistema de vCenter Server mediante vSphere Web Client.

2 En la página de inicio de vSphere Web Client, haga clic en **Administración**.

3 En **Configuración del sistema**, haga clic en **Servicios**.

4 Seleccione **Servicio de ImageBuilder**, haga clic en el menú **Acciones** y seleccione **Editar tipo de inicio**.

   - En Windows, el servicio de vSphere ESXi Image Builder se encuentra deshabilitado. En la ventana **Editar tipo de inicio**, seleccione **Manual** o **Automático** para habilitar Auto Deploy.
   - En vCenter Server Appliance, el servicio vSphere ESXi Image Builder está establecido como **Manual** de manera predeterminada. Si desea que el servicio se inicie de manera automática durante el arranque del sistema operativo, seleccione **Automático**.

   Si selecciona el tipo de inicio manual, debe iniciar el servicio manualmente después del arranque del sistema operativo cada vez que desee usar el servicio.

5 (opcional) Haga clic en el icono **Iniciar el servicio**.

6 (opcional) Si desea utilizar vSphere ESXi Image Builder con vSphere Web Client, cierre sesión en vSphere Web Client y vuelva a iniciar sesión.

   El icono **Auto Deploy** es visible en la página de inicio de vSphere Web Client.

Pasos siguientes

- Agregar un almacén de software.

- Importar un almacén de software.
- Clonar un perfil de imagen.
- Crear un perfil de imagen.

Usar los cmdlets de vSphere ESXi Image Builder

Los cmdlets de vSphere ESXi Image Builder se implementan como cmdlets de Microsoft PowerShell y se incluyen en PowerCLI. Los usuarios de los cmdlets de vSphere ESXi Image Builder pueden aprovechar todas las funciones de PowerCLI.

Los usuarios experimentados de PowerShell pueden utilizar los cmdlets de vSphere ESXi Image Builder al igual que otros cmdlets de PowerShell. Si estos son sus primeros pasos con PowerShell y PowerCLI, siga estos consejos.

Puede escribir cmdlets, parámetros y valores de parámetros en el shell de PowerCLI.

- Obtenga ayuda para cualquier cmdlet a través de `Get-Help` *`cmdlet_name`*.
- Recuerde que PowerShell no distingue mayúsculas de minúsculas.
- Utilice la opción de finalización con tabulación para los nombres de cmdlets y parámetros.
- Formatee cualquier variable y salida de cmdlet utilizando `Format-List` o `Format-Table` o sus formas cortas `fl` o `ft`. Consulte `Get-Help Format-List`.
- Utilice caracteres comodín para la búsqueda y filtrado de VIB y perfiles de imagen. Son compatibles todas las expresiones con comodines.

Transmitir parámetros por nombre

Puede transmitir parámetros por nombre en la mayoría de los casos y rodear los valores de parámetros que contienen espacios o caracteres especiales con comillas dobles.

```
Add-EsxSoftwarePackage -ImageProfile profile42 -SoftwarePackage "partner package 35"
```

Transmitir parámetros como objetos

Puede pasar los parámetros como objetos si desea realizar el scripting y automatización. Puede utilizar la técnica con cmdlets que devuelven varios objetos o con cmdlets que devuelven un solo objeto.

1. Asocie la salida de un cmdlet que devuelve varios objetos a una variable.

   ```
   $profs = Get-EsxImageProfile
   ```

2. Cuando ejecute el cmdlet que necesita el objeto como entrada, acceda al objeto por posición, con la lista comenzando con 0.

   ```
   Add-EsxSoftwarePackage -ImageProfile $profs[4] -SoftwarePackage partner-pkg
   ```

El ejemplo agrega el paquete de software especificado al quinto perfil de imagen de la lista devuelto por `Get-EsxImageProfile`.

La mayoría de los ejemplos de la documentación *Instalar y configurar vSphere* pasan los parámetros por nombre. Flujos de trabajo de vSphere ESXi Image Builder incluye ejemplos que pasan parámetros como objetos.

Usar vSphere ESXi Image Builder con vSphere Web Client

Puede administrar paquetes de software (VIB), perfiles de imagen y almacenes de software mediante el servicio vSphere ESXi Image Builder en vSphere Web Client.

- Agregar un almacén de software

  Para poder trabajar con almacenes de software y personalizar perfiles de imagen, debe agregar uno o varios almacenes de software al inventario de vSphere ESXi Image Builder. Puede agregar un almacén de software utilizando vSphere Web Client.

- Importar un almacén de software

  Si hay un almacén sin conexión ubicado en su sistema de archivos local, puede importar el archivo ZIP al inventario de vSphere ESXi Image Builder mediante vSphere Web Client.

- Clonar un perfil de imagen

  Puede utilizar vSphere Web Client para clonar perfiles de imagen. Puede clonar un perfil de imagen cuando quiera realizar pequeños cambios en la lista de VIB de un perfil; o si quiere utilizar hosts de distintos proveedores y quiere utilizar el mismo perfil básico, pero desea agregar VIB específicos de los proveedores.

- Crear un perfil de imagen

  Puede crear un nuevo perfil de imagen a través de vSphere Web Client en lugar de clonar uno existente. Podría considerar crear un nuevo perfil de imagen si este difiere de forma significativa de los perfiles de imagen de su inventario.

- Editar un perfil de imagen

  Puede editar perfiles de imagen mediante vSphere Web Client. Puede cambiar el nombre, los detalles y la lista VIB de un perfil de imagen.

- Comparar perfiles de imagen

  Puede comparar dos perfiles de imagen a través de vSphere Web Client, por ejemplo, para comprobar si poseen la misma lista de VIB, versión o nivel de aceptación.

- Mover un perfil de imagen a un almacén de software distinto

  Puede mover perfiles de imagen entre almacenes personalizados mediante vSphere Web Client. Puede mover un perfil de imagen a un almacén personalizado para editar el perfil de imagen.

- Exportar un perfil de imagen a ISO o ZIP de paquete sin conexión

  Puede exportar un perfil de imagen a una imagen ISO o un archivo ZIP mediante vSphere Web Client. Puede utilizar la imagen ISO como instalador de ESXi o para actualizar los hosts con vSphere Upgrade Manager. El archivo ZIP contiene metadatos y los VIB del perfil de imagen. Puede utilizarlo para las actualizaciones de ESXi o como almacén sin conexión.

Agregar un almacén de software

Para poder trabajar con almacenes de software y personalizar perfiles de imagen, debe agregar uno o varios almacenes de software al inventario de vSphere ESXi Image Builder. Puede agregar un almacén de software utilizando vSphere Web Client.

Requisitos previos

Compruebe que el servicio vSphere ESXi Image Builder esté habilitado y en ejecución. Consulte Configurar el tipo de inicio del servicio vSphere ESXi Image Builder.

Procedimiento

1 En la página de inicio de vSphere Web Client, haga clic en **Auto Deploy**.

  De manera predeterminada, solo la función de administrador incluye privilegios para usar el servicio de vSphere ESXi Image Builder .

2 En la pestaña **Almacenes de software**, haga clic en el icono **Agregar almacén de software**.

3 Seleccione el tipo de almacén que desea crear.

Opción	Acción
Almacén en línea	a Introduzca el nombre del almacén en el inventario. b Introduzca la URL en el almacén en línea.
Almacén personalizado	Introduzca el nombre del almacén en el inventario.

4 Haga clic en **Aceptar**.

Pasos siguientes

- Puede asociar un perfil de imagen con una nueva regla de vSphere Auto Deploy para aprovisionar hosts ESXi. Consulte Crear una regla de implementación o Clonar una regla de implementación.
- Puede asociar un perfil de imagen con un host ESXi. Consulte Agregar un host al inventario de vSphere Auto Deploy.
- Editar la asociación de perfil de imagen de un host.

Importar un almacén de software

Si hay un almacén sin conexión ubicado en su sistema de archivos local, puede importar el archivo ZIP al inventario de vSphere ESXi Image Builder mediante vSphere Web Client.

Requisitos previos

Compruebe que el servicio vSphere ESXi Image Builder esté habilitado y en ejecución. Consulte Configurar el tipo de inicio del servicio vSphere ESXi Image Builder.

Procedimiento

1 En la página de inicio de vSphere Web Client, haga clic en **Auto Deploy**.

   De manera predeterminada, solo la función de administrador incluye privilegios para usar el servicio de vSphere ESXi Image Builder .

2 En la pestaña **Almacenes de software**, haga clic en el icono **Importar almacén de software**.

3 Introduzca el nombre del almacén de software en el inventario.

4 Haga clic en **Examinar** y seleccione un archivo ZIP en el sistema local que contenga el almacén de software al que desea realizar la importación.

5 Haga clic en **Cargar**.

Pasos siguientes

- Puede asociar un perfil de imagen con una nueva regla de vSphere Auto Deploy para aprovisionar hosts ESXi. Consulte Crear una regla de implementación o Clonar una regla de implementación.
- Puede asociar un perfil de imagen con un host ESXi. Consulte Agregar un host al inventario de vSphere Auto Deploy.
- Editar la asociación de perfil de imagen de un host.

Clonar un perfil de imagen

Puede utilizar vSphere Web Client para clonar perfiles de imagen. Puede clonar un perfil de imagen cuando quiera realizar pequeños cambios en la lista de VIB de un perfil; o si quiere utilizar hosts de distintos proveedores y quiere utilizar el mismo perfil básico, pero desea agregar VIB específicos de los proveedores.

El nivel de aceptación de los VIB que se agregan a la imagen de base debe ser al menos tan alto como el de la imagen de base. Si agrega un VIB con un nivel de aceptación inferior al del perfil de imagen, debe reducir el nivel de aceptación del perfil de imagen. Para obtener más información, consulte Trabajar con niveles de aceptación.

Requisitos previos

- Compruebe que el servicio vSphere ESXi Image Builder esté habilitado y en ejecución. Consulte Configurar el tipo de inicio del servicio vSphere ESXi Image Builder.
- Agregue o importe un almacén de software al inventario de vSphere ESXi Image Builder. Consulte Agregar un almacén de software y Importar un almacén de software.

Procedimiento

1 En la página de inicio de vSphere Web Client, haga clic en **Auto Deploy**.

   De manera predeterminada, solo la función de administrador incluye privilegios para usar el servicio de vSphere ESXi Image Builder .

2 En la pestaña **Almacenes de software**, seleccione el almacén de software en el que se encuentra el perfil de imagen que desea utilizar.

3 En la lista de perfiles de imagen del almacén, seleccione el perfil de imagen que desea clonar y haga clic en **Clonar**.

4 Escriba un nombre de perfil de imagen, un proveedor y una descripción.

   Debe escribir un nombre de perfil de imagen exclusivo.

5 En la lista desplegable **Almacén de software**, seleccione el almacén personalizado al que desea agregar el nuevo perfil de imagen y haga clic en **Siguiente**.

6 (opcional) En la lista desplegable, seleccione un nivel de aceptación para el perfil de imagen.

7 En la pestaña **Disponible**, seleccione los VIB que desea agregar al perfil de imagen y anule la selección de los VIB que desea quitar.

   Para ver los VIB que se agregarán al perfil de imagen, consulte la pestaña **Seleccionado**. Puede filtrar los VIB por almacén de software en la lista desplegable **Almacén de software** de la pestaña **Disponible**.

   Nota El perfil de imagen debe contener una imagen de ESXi de arranque para ser válido.

8 Haga clic en **Siguiente**.

   vSphere ESXi Image Builder verifica que el cambio no invalide el perfil. Algunos VIB dependen de otros VIB y pierden su validez si se incluyen en un perfil de imagen por separado. Cuando se agrega o se quita un VIB, vSphere ESXi Image Builder comprueba si se cumplen las dependencias del paquete.

9 En la página Listo para finalizar, revise la información de resumen del nuevo perfil de imagen y haga clic en **Finalizar**.

Pasos siguientes

- Puede asociar un perfil de imagen con una nueva regla de vSphere Auto Deploy para aprovisionar hosts ESXi. Consulte Crear una regla de implementación o Clonar una regla de implementación.
- Puede asociar un perfil de imagen con un host ESXi. Consulte Agregar un host al inventario de vSphere Auto Deploy.
- Editar la asociación de perfil de imagen de un host.

Crear un perfil de imagen

Puede crear un nuevo perfil de imagen a través de vSphere Web Client en lugar de clonar uno existente. Podría considerar crear un nuevo perfil de imagen si este difiere de forma significativa de los perfiles de imagen de su inventario.

El nivel de aceptación de los VIB que se agregan a la imagen de base debe ser al menos tan alto como el de la imagen de base. Si agrega un VIB con un nivel de aceptación inferior al del perfil de imagen, debe reducir el nivel de aceptación del perfil de imagen. Para obtener más información, consulte Trabajar con niveles de aceptación.

Requisitos previos

- Compruebe que el servicio vSphere ESXi Image Builder esté habilitado y en ejecución. Consulte Configurar el tipo de inicio del servicio vSphere ESXi Image Builder.
- Agregue o importe un almacén de software al inventario de vSphere ESXi Image Builder. Consulte Agregar un almacén de software y Importar un almacén de software.

Procedimiento

1 En la página de inicio de vSphere Web Client, haga clic en **Auto Deploy**.

   De manera predeterminada, solo la función de administrador incluye privilegios para usar el servicio de vSphere ESXi Image Builder .

2 En la pestaña **Almacenes de software**, seleccione el almacén personalizado en el que desea crear un nuevo perfil de imagen.

3 En la pestaña Perfiles de imagen, haga clic en **Nuevo perfil de imagen**.

4 Escriba un nombre de perfil de imagen, un proveedor y una descripción.

   Debe escribir un nombre de perfil de imagen exclusivo.

5 En la lista desplegable **Almacén de software**, seleccione el almacén personalizado al que desea agregar el nuevo perfil de imagen y haga clic en **Siguiente**.

6 (opcional) En la lista desplegable, seleccione un nivel de aceptación para el perfil de imagen.

7 En la pestaña **Disponible**, seleccione los VIB que desea agregar al perfil de imagen y anule la selección de los VIB que desea quitar.

   Para ver los VIB que se agregarán al perfil de imagen, consulte la pestaña **Seleccionado**. Puede filtrar los VIB por almacén de software en la lista desplegable **Almacén de software** de la pestaña **Disponible**.

   Nota El perfil de imagen debe contener una imagen de ESXi de arranque para ser válido.

8 Haga clic en **Siguiente**.

   vSphere ESXi Image Builder verifica que el cambio no invalide el perfil. Algunos VIB dependen de otros y no serán válidos si no los incluye en un perfil de imagen de forma separada. Cuando se agrega o se quita un VIB, vSphere ESXi Image Builder comprueba que se cumplan las dependencias del paquete.

9 En la página Listo para finalizar, revise la información de resumen del nuevo perfil de imagen y haga clic en **Finalizar**.

Pasos siguientes

- Puede asociar un perfil de imagen con una nueva regla de vSphere Auto Deploy para aprovisionar hosts ESXi. Consulte Crear una regla de implementación o Clonar una regla de implementación.
- Puede asociar un perfil de imagen con un host ESXi. Consulte Agregar un host al inventario de vSphere Auto Deploy.
- Editar la asociación de perfil de imagen de un host.

Editar un perfil de imagen

Puede editar perfiles de imagen mediante vSphere Web Client. Puede cambiar el nombre, los detalles y la lista VIB de un perfil de imagen.

El nivel de aceptación de los VIB que se agregan a la imagen de base debe ser al menos tan alto como el de la imagen de base. Si agrega un VIB con un nivel de aceptación inferior al del perfil de imagen, debe reducir el nivel de aceptación del perfil de imagen. Para obtener más información, consulte Trabajar con niveles de aceptación.

Requisitos previos

- Compruebe que el servicio vSphere ESXi Image Builder esté habilitado y en ejecución. Consulte Configurar el tipo de inicio del servicio vSphere ESXi Image Builder.
- Agregue o importe un almacén de software al inventario de vSphere ESXi Image Builder. Consulte Agregar un almacén de software y Importar un almacén de software.
- Compruebe que exista al menos un almacén personalizado en el inventario de vSphere ESXi Image Builder .

Procedimiento

1. En la página de inicio de vSphere Web Client, haga clic en **Auto Deploy**.

   De manera predeterminada, solo la función de administrador incluye privilegios para usar el servicio de vSphere ESXi Image Builder .
2. En la pestaña **Almacenes de software**, seleccione el almacén de software en el que se encuentra el perfil de imagen que desea utilizar.
3. En la pestaña **Perfiles de imagen**, seleccione el perfil de imagen que desea editar y haga clic en **Editar**.
4. (opcional) Cambie el nombre, el proveedor y la información de la descripción del perfil de imagen.
5. Haga clic en **Siguiente**.

6 En la pestaña **Disponible**, seleccione los VIB que desea agregar al perfil de imagen y anule la selección de los VIB que desea quitar.

   Para ver los VIB que se agregarán al perfil de imagen, consulte la pestaña **Seleccionado**. Puede filtrar los VIB por almacén de software en la lista desplegable **Almacén de software** de la pestaña **Disponible**.

   Nota El perfil de imagen debe contener una imagen de ESXi de arranque para ser válido.

7 Haga clic en **Siguiente**.

   vSphere ESXi Image Builder verifica que el cambio no invalide el perfil. Algunos VIB dependen de otros VIB y pierden su validez si se incluyen en un perfil de imagen por separado. Cuando se agrega o se quita un VIB, vSphere ESXi Image Builder comprueba si se cumplen las dependencias del paquete.

8 En la página Listo para finalizar, revise la información del resumen del perfil de imagen editado y haga clic en **Finalizar**.

Pasos siguientes

- Puede asociar un perfil de imagen con una nueva regla de vSphere Auto Deploy para aprovisionar hosts ESXi. Consulte Crear una regla de implementación o Clonar una regla de implementación.
- Puede asociar un perfil de imagen con un host ESXi. Consulte Agregar un host al inventario de vSphere Auto Deploy.
- Editar la asociación de perfil de imagen de un host.

Comparar perfiles de imagen

Puede comparar dos perfiles de imagen a través de vSphere Web Client, por ejemplo, para comprobar si poseen la misma lista de VIB, versión o nivel de aceptación.

Requisitos previos

- Compruebe que el servicio vSphere ESXi Image Builder esté habilitado y en ejecución. Consulte Configurar el tipo de inicio del servicio vSphere ESXi Image Builder.
- Agregue o importe un almacén de software al inventario de vSphere ESXi Image Builder. Consulte Agregar un almacén de software y Importar un almacén de software.

Procedimiento

1 En la página de inicio de vSphere Web Client, haga clic en **Auto Deploy**.

   De manera predeterminada, solo la función de administrador incluye privilegios para usar el servicio de vSphere ESXi Image Builder .

2 En la pestaña **Almacenes de software**, seleccione el almacén de software en el que se encuentra el perfil de imagen que desea utilizar.

3 En la pestaña **Perfiles de imagen**, seleccione el perfil de imagen que desea comparar y haga clic en **Comparar con**.

4 En el cuadro de diálogo Comparar perfiles de imagen, en el menú desplegable **Almacén de software**, seleccione el almacén de software que contenga el segundo perfil de imagen que quiere comparar.

5 En el menú desplegable **Perfil de imagen**, seleccione el segundo perfil de imagen que quiera comparar.

6 En Paquetes de software, en la pestaña **Todo**, vea la comparación de los dos perfiles de imagen.

   En la parte izquierda de la lista aparecen los nombres, versiones, niveles de aceptación y proveedores de los VIB que contiene el primer perfil de imagen seleccionado. En la parte derecha de la lista se proporciona información sobre el segundo perfil de imagen. Los VIB marcados con `sin cambio` son iguales en ambos perfiles. Los VIB que están presentes en uno solo de los perfiles de imagen se marcan como `faltante` en el perfil de imagen en el que no se incluyen.

Mover un perfil de imagen a un almacén de software distinto

Puede mover perfiles de imagen entre almacenes personalizados mediante vSphere Web Client. Puede mover un perfil de imagen a un almacén personalizado para editar el perfil de imagen.

Requisitos previos

- Compruebe que el servicio vSphere ESXi Image Builder esté habilitado y en ejecución. Consulte Configurar el tipo de inicio del servicio vSphere ESXi Image Builder.
- Agregue o importe un almacén de software al inventario de vSphere ESXi Image Builder. Consulte Agregar un almacén de software y Importar un almacén de software.
- Compruebe que exista al menos un almacén personalizado en el inventario de vSphere ESXi Image Builder .

Procedimiento

1 En la página de inicio de vSphere Web Client, haga clic en **Auto Deploy**.

   De manera predeterminada, solo la función de administrador incluye privilegios para usar el servicio de vSphere ESXi Image Builder .

2 En la pestaña **Almacenes de software**, seleccione el almacén de software en el que se encuentra el perfil de imagen que desea utilizar.

3 En la pestaña **Perfiles de imagen**, seleccione uno de ellos y haga clic en **Mover a**.

4 En la lista desplegable, seleccione el almacén personalizado al que desea mover el perfil de imagen.

5 Haga clic en **Aceptar**.

Exportar un perfil de imagen a ISO o ZIP de paquete sin conexión

Puede exportar un perfil de imagen a una imagen ISO o un archivo ZIP mediante vSphere Web Client. Puede utilizar la imagen ISO como instalador de ESXi o para actualizar los hosts con vSphere Upgrade Manager. El archivo ZIP contiene metadatos y los VIB del perfil de imagen. Puede utilizarlo para las actualizaciones de ESXi o como almacén sin conexión.

Requisitos previos

- Compruebe que el servicio vSphere ESXi Image Builder esté habilitado y en ejecución. Consulte Configurar el tipo de inicio del servicio vSphere ESXi Image Builder.
- Agregue o importe un almacén de software al inventario de vSphere ESXi Image Builder. Consulte Agregar un almacén de software y Importar un almacén de software.

Procedimiento

1 En la página de inicio de vSphere Web Client, haga clic en **Auto Deploy**.

   De manera predeterminada, solo la función de administrador incluye privilegios para usar el servicio de vSphere ESXi Image Builder .

2 En la pestaña **Almacenes de software**, seleccione el almacén de software en el que se encuentra el perfil de imagen que desea utilizar.

3 En la pestaña **Perfiles de imagen**, seleccione el perfil de imagen que desea exportar y haga clic en **Exportar perfil de imagen**.

4 Seleccione el tipo del archivo exportado.

Opción	Descripción
ISO	Exporta el perfil de imagen a una imagen ISO de arranque. Si desea crear una imagen ISO que se pueda grabar en un CD o DVD, y que se pueda utilizar para arrancar una instancia de ESXi sin estado, active la casilla **No incluya un instalador en la imagen ISO**.
ZIP	Exporta el perfil de imagen a un archivo ZIP.

5 (opcional) Si desea omitir la verificación del nivel de aceptación del perfil de imagen, seleccione **Omitir comprobación de firma de perfil de imagen**.

6 Haga clic en el botón **Generar imagen**.

7 Cuando la imagen se genere correctamente, haga clic en **Descargar** para descargar el archivo exportado.

8 Haga clic en **Cerrar**.

Usar los cmdlets de PowerCLI de vSphere ESXi Image Builder

Los cmdlets de vSphere ESXi Image Builder permiten manipular almacenes de software, perfiles de imagen y VIB.

Clonar un perfil de imagen

La clonación de un perfil publicado es la manera más sencilla de crear un perfil de imagen personalizado. La clonación de un perfil resulta especialmente útil si desea eliminar algunos VIB puntuales de un perfil, o si desea usar hosts de diferentes proveedores y quiere usar el mismo perfil básico, pero también agregar VIB de proveedores específicos. Las grandes instalaciones o los partners de VMware pueden considerar la posibilidad de crear un nuevo perfil.

Requisitos previos

- Instalar PowerCLI y todo el software necesario como requisito previo. Consulte Instalar y usar vSphere ESXi Image Builder.
- Compruebe que tenga acceso al almacén de software que contiene el perfil de imagen que desea clonar.

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Add-EsxSoftwareDepot` para cada almacén con el que desea trabajar.

Opción	Acción
Almacén remoto	Ejecute `Add-EsxSoftwareDepot -DepotUrl` *depot_url*.
Archivo ZIP	a Descargue el archivo ZIP en un sistema de archivos local. b Ejecute `Add-EsxSoftwareDepot -DepotUrl C:\file_path\`*offline-bundle*`.zip`.

El cmdlet devuelve uno o más objetos `SoftwareDepot`.

2 (opcional) Ejecute el cmdlet `Get-EsxImageProfile` para buscar el nombre del perfil que desea clonar.

Puede utilizar opciones de filtros con `Get-EsxImageProfile`.

3 Ejecute el cmdlet `New-EsxImageProfile` para crear un nuevo perfil y use el parámetro `-CloneProfile` para especificar el perfil que desea clonar.

```
New-EsxImageProfile -CloneProfile My_Profile -Name "Test Profile 42"
```

En este ejemplo, se clona el perfil denominado *My_ Profile* y se asigna el nombre Test Profile 42. Debe especificar una combinación exclusiva de nombre y proveedor para el perfil clonado.

Pasos siguientes

Consulte Revisar contenido de almacenes para ver algunos ejemplos de filtros.

Personalice el perfil de imagen agregando o eliminando VIB. Consulte Agregar VIB a un perfil de imagen.

Agregar VIB a un perfil de imagen

Puede agregar uno o más VIB a un perfil de imagen si dicho perfil de imagen no está configurado en solo lectura. Si el nuevo VIB depende de otros VIB o entra en conflicto con otros VIB del perfil, aparecerá un mensaje en el símbolo del sistema de PowerShell y no se agregará el VIB.

Puede agregar VIB desde VMware o desde partners de VMware a un perfil de imagen. Si agrega VIB de VMware, vSphere ESXi Image Builder realiza la validación. Si agrega VIB desde uno o más partners OEM de forma simultánea, no se informa de errores, pero el perfil de imagen resultante podría no funcionar. Instale los VIB desde solo un proveedor OEM al mismo tiempo.

Si aparece un error sobre problemas con el nivel de aceptación, cambie el nivel de aceptación del perfil de imagen y el nivel de aceptación del host. Considere meticulosamente si es apropiado el cambio del nivel de aceptación del host. Los niveles de aceptación de VIB se establecen durante la creación del VIB y no se pueden cambiar.

Puede agregar los VIB incluso si el perfil de imagen resultante no es válido.

Nota VMware solo puede admitir entornos y configuraciones que hayan demostrado ser estables y totalmente funcionales a través de pruebas rigurosas y exhaustivas. Utilice solo aquellas configuraciones compatibles. Puede utilizar VIB personalizados si reduce el nivel de aceptación del host y, como resultado, la compatibilidad. En dicho caso, registre los cambios realizados, a fin de que pueda revertirlos en caso de que desee eliminar los VIB personalizados y restaurar posteriormente el nivel de aceptación del host al valor predeterminado (Partner Supported). Consulte Trabajar con niveles de aceptación.

Requisitos previos

Instalar PowerCLI y todo el software necesario como requisito previo. Consulte Instalar vSphere ESXi Image Builder y software de requisito previo

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Add-EsxSoftwareDepot` para cada almacén con el que desea trabajar.

Opción	Acción
Almacén remoto	Ejecute `Add-EsxSoftwareDepot -DepotUrl` *`depot_url`*.
Archivo ZIP	a Descargue el archivo ZIP en un sistema de archivos local. b Ejecute `Add-EsxSoftwareDepot -DepotUrl C:\file_path\`*`offline-bundle`*`.zip`.

El cmdlet devuelve uno o más objetos `SoftwareDepot`.

2 Ejecute el cmdlet `Get-EsxImageProfile` para mostrar todos los perfiles de imagen de todos los almacenes actualmente visibles.

El cmdlet devuelve todos los perfiles disponibles. Puede limitar la búsqueda utilizando los argumentos opcionales para filtrar la salida.

3 Clone el perfil.

```
New-EsxImageProfile -CloneProfile My_Profile -Name "Test Profile 42" -Vendor "My Vendor"
```

Los perfiles de imagen publicados por VMware y sus partners son de solo lectura. Para realizar cambios, deberá clonar el perfil de imagen. Se requiere el parámetro `vendor`.

4 Ejecute el cmdlet `Add-EsxSoftwarePackage` para agregar un paquete nuevo a uno de los perfiles de imagen.

```
Add-EsxSoftwarePackage -ImageProfile My_Profile -SoftwarePackage partner-package
```

El cmdlet ejecuta las pruebas de validación estándares en el perfil de imagen. Si la validación es correcta, el cmdlet devuelve un perfil de imagen modificado y validado. Si el VIB que desea agregar depende de un VIB diferente, el cmdlet muestra dicha información e incluye el VIB que resolvería la dependencia. Si el nivel de aceptación del VIB que desea agregar es inferior al nivel de aceptación del perfil de imagen, ocurrirá un error.

Exportar un perfil de imagen a ISO o ZIP de paquete sin conexión

Puede exportar un perfil de imagen a una imagen ISO o un archivo ZIP que contenga archivos y carpetas de componentes. No puede crear los dos si ejecuta el cmdlet una sola vez. Puede utilizar una imagen ISO como el instalador de ESXi o cargar la imagen ISO a vSphere Update Manager para actualizaciones. Puede utilizar el archivo ZIP, que contiene metadatos y los VIB especificados en el perfil de imagen, para actualizar a ESXi 5.0 y posterior.

Requisitos previos

Instalar PowerCLI y todo el software necesario como requisito previo. Consulte Instalar vSphere ESXi Image Builder y software de requisito previo.

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Add-EsxSoftwareDepot` para cada almacén con el que desea trabajar.

Opción	Acción
Almacén remoto	Ejecute `Add-EsxSoftwareDepot -DepotUrl` *depot_url*.
Archivo ZIP	a Descargue el archivo ZIP en un sistema de archivos local. b Ejecute `Add-EsxSoftwareDepot -DepotUrl C:\file_path\`*offline-bundle*`.zip`.

El cmdlet devuelve uno o más objetos `SoftwareDepot`.

2 Ejecute `Export-EsxImageProfile` para exportar el perfil de imagen.

Formato de exportación	Cmdlet
Imágenes ISO	`Export-EsxImageProfile` con el parámetro `-ExportToIso`
Archivos ZIP de almacén sin conexión	`Export-EsxImageProfile` con el parámetro `-ExportToBundle`

Resultados

Para la imagen ISO, vSphere ESXi Image Builder valida firmas de VIB, agrega archivos binarios de VIB a la imagen y descarga la imagen a la ubicación especificada. Para el archivo ZIP, vSphere ESXi Image Builder valida firmas de VIB y descarga los archivos binarios de VIB a la ubicación especificada.

Ejemplo: Exportar un perfil de imagen

Siga estos pasos para exportar un perfil de imagen a una imagen ISO.

1 Agregue el almacén de software.

```
Add-EsxSoftwareDepot -DepotUrl url_or_file
```

2 Observe todos los perfiles de imagen disponibles para encontrar el nombre del perfil de imagen que desea exportar.

```
Get-EsxImageProfile
```

3 Exporte el perfil de imagen.

```
Export-EsxImageProfile -ImageProfile "myprofile" -ExportToIso -FilePath iso_name
```

Siga estos pasos para exportar un perfil de imagen a un archivo ZIP que contenga archivos y carpetas de componentes.

1 Agregue el almacén de software.

```
Add-EsxSoftwareDepot -DepotUrl url_or_file
```

2 Observe todos los perfiles de imagen disponibles para encontrar el nombre del perfil de imagen que desea exportar.

```
Get-EsxImageProfile
```

3 Exporte el perfil de imagen.

```
Export-EsxImageProfile -ImageProfile "myprofile" -ExportToBundle -FilePath C:\my_bundle.zip
```

Pasos siguientes

Utilice la imagen ISO en una instalación de ESXi o cargue la imagen ISO a vSphereUpdate Manager para realizar actualizaciones.

Utilice el archivo ZIP para actualizar una instalación de ESXi.

- Importe el archivo ZIP a vSphere Update Manager para utilizarlo con líneas base de revisión.
- Descargue el archivo ZIP a un host ESXi o un almacén de datos, y ejecute los comandos `esxcli software vib` para importar los VIB del archivo ZIP.

Consulte la documentación de *Actualizar vSphere*.

Mantenimiento de perfiles de imagen entre sesiones

Cuando se crea un perfil de imagen y se sale de la sesión de PowerCLI, el perfil de imagen ya no está disponible cuando se inicia una nueva sesión. Puede exportar el perfil de imagen a un almacén de software de archivos zip y agregar ese depósito en la siguiente sesión.

Requisitos previos

Instalar PowerCLI y todo el software necesario como requisito previo. Consulte Instalar vSphere ESXi Image Builder y software de requisito previo.

Procedimiento

1. En una sesión de PowerCLI, cree un perfil de imagen, por ejemplo, clonando un perfil de imagen existente y agregando un VIB.
2. Exporte el perfil de imagen a un archivo ZIP llamando a `Export-EsxImageProfile` con el parámetro `ExportToBundle`.

   ```
   Export-EsxImageProfile    -ImageProfile "my_profile" -ExportToBundle -FilePath
                   "C:\isos\temp-base-plus-vib25.zip"
   ```

3. Salga de la sesión de PowerCLI.
4. Cuando inicie una nueva sesión de PowerCLI, agregue el almacén que contiene su perfil de imagen para poder acceder a él.

   ```
   Add-EsxSoftwareDepot "C:\isos\temp-base-plus-vib25.zip"
   ```

Comparar perfiles de imagen

Puede comparar dos perfiles de imagen a través del cmdlet `Compare-EsxImageProfile`, por ejemplo, para comprobar si poseen la misma lista de VIB o nivel de aceptación. También es posible la comparación de perfiles de imagen o sus propiedades utilizando los operadores de comparación de PowerShell.

Requisitos previos

Instalar PowerCLI y todo el software necesario como requisito previo. Consulte Instalar vSphere ESXi Image Builder y software de requisito previo.

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Add-EsxSoftwareDepot` para cada almacén con el que desea trabajar.

Opción	Acción
Almacén remoto	Ejecute `Add-EsxSoftwareDepot -DepotUrl` *`depot_url`*.
Archivo ZIP	a Descargue el archivo ZIP en un sistema de archivos local. b Ejecute `Add-EsxSoftwareDepot -DepotUrl C:\file_path\`*`offline-bundle`*`.zip`.

El cmdlet devuelve uno o más objetos `SoftwareDepot`.

2 (opcional) Ejecute el cmdlet `Get-EsxImageProfile` para visualizar una lista de todos los perfiles de imagen en todos los almacenes disponibles.

En la lista, puede encontrar los nombres de los perfiles de imagen que desea comparar.

3 Antes de comparar los perfiles de imagen, asígnelos a variables.

Por ejemplo, puede crear las variables `$imageProfile1` y `$imageProfile2` para conservar los nombres de los perfiles de imagen comparados.

```
$imageProfile1
                = Get-EsxImageProfile -Name "ImageProfile1"
$imageProfile2
                = Get-EsxImageProfile -Name "ImageProfile2"
```

4 Compare los dos perfiles de imagen a través del cmdlet `Compare-EsxImageProfile` o el operador de comparación `-eq`, que devuelve un valor booleano.

- Compare los dos perfiles de imagen para obtener una descripción completa de las diferencias a través del cmdlet `Compare-EsxImageProfile`.

```
Compare-EsxImageProfile -ReferenceProfile
                     $imageProfile1 -ComparisonProfile $imageProfile2
```

- Compare los dos perfiles de imagen por lista de VIB y nivel de aceptación a través del operador de comparación `-eq`.

```
    if ($imageProfile1 -eq $imageProfile2) {
       Write-host "Successfully verified that both image profiles are equal."
    } else {
       Write-host "Failed to verify that the image profiles are equal."
    }
```

- Compare los dos perfiles de imagen por una propiedad específica a través del operador de comparación `-eq`.

```
if ($imageProfile1.vendor -eq $imageProfile2.vendor) {
   Write-host "Successfully verified that both image profiles are equal."
} else {
   Write-host "Failed to verify that the image profiles are equal."
}
```

Comparar VIB

Puede comparar dos VIB o sus propiedades usando los operadores de comparación de PowerShell.

Requisitos previos

Instalar PowerCLI y todo el software necesario como requisito previo. Consulte Instalar vSphere ESXi Image Builder y software de requisito previo.

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Add-EsxSoftwareDepot` para cada almacén con el que desea trabajar.

Opción	Acción
Almacén remoto	Ejecute `Add-EsxSoftwareDepot -DepotUrl` *`depot_url`*.
Archivo ZIP	a Descargue el archivo ZIP en un sistema de archivos local. b Ejecute `Add-EsxSoftwareDepot -DepotUrl C:\file_path\`*`offline-bundle`*`.zip`.

El cmdlet devuelve uno o más objetos `SoftwareDepot`.

2 (opcional) Ejecute el cmdlet `Get-EsxSoftwarePackage` para ver todos los VIB disponibles.

En la lista, puede encontrar los nombres de los VIB que desea comparar.

3 Antes de comparar los VIB, asígnelos a variables.

Por ejemplo, puede crear las variables `$vib1` y `$vib2` para mantener los nombre de los VIB comparados.

```
$vib1 = Get-EsxSoftwarePackage -Name "ReferenceVIB"
$vib2 = Get-EsxSoftwarePackage -Name "ComparisonVIB"
```

4 Use un operador de comparación para comparar los VIB por contenido y nivel de aceptación, o por una propiedad específica.

- Compare los dos VIB según su contenido y nivel de aceptación.

```
if ($vib1 -eq $vib2) {
   Write-host "Successfully verified that both VIBs are equal."
} else {
   Write-host "Failed to verify that the VIBs are equal."
}
```

- Compare una propiedad específica de los VIB usando un operador de comparaciones, como `-eq`, `-lt`, `-le`, `-gt` o `-ge`.

```
if ($vib1.VersionObject -lt $vib2.VersionObject) {
   Write-host "Successfully verified that both the VIBs are equal."
} else {
   Write-host "Failed to verify that the VIBs are equal."
}
```

Trabajar con niveles de aceptación

Los hosts, los perfiles de imagen y los VIB individuales tienen niveles de aceptación. Los niveles de aceptación de VIB muestran cómo se probó el VIB. Como parte importante de los procedimientos de instalación y actualización, es necesario que comprenda lo que significa cada nivel de aceptación, cómo cambiar los niveles y qué implica cada cambio.

Los niveles de aceptación se configuran para hosts, perfiles de imagen y VIB individuales. El nivel de aceptación predeterminado para una imagen o un perfil de imagen de ESXi es PartnerSupported.

Niveles de aceptación de host

El nivel de aceptación de host determina qué VIB puede instalar en un host. Puede cambiar el nivel de aceptación de un host mediante los comandos ESXCLI. De forma predeterminada, los hosts ESXi tienen el nivel de aceptación PartnerSupported para permitir que se realicen actualizaciones fácilmente con los VIB PartnerSupported.

Nota VMware admite hosts con el nivel de aceptación PartnerSupported. Para conocer los problemas que podrían surgir con los VIB individuales con nivel de aceptación PartnerSupported, póngase en contacto con la organización de soporte del partner.

Niveles de aceptación de perfil de imagen

El nivel de aceptación de perfil de imagen se establece en el nivel de aceptación de VIB más bajo que haya en el perfil. Si desea agregar un VIB con un nivel de aceptación bajo a un perfil de imagen, puede cambiar el nivel de aceptación del perfil con el cmdlet `Set-EsxImageProfile`. Consulte Establecer el nivel de aceptación del perfil de imagen.

vSphere Update Manager no muestra el nivel de aceptación real. Utilice cmdlets de vSphere ESXi Image Builder para recuperar la información de nivel de aceptación para VIB y perfiles de imagen.

Niveles de aceptación de VIB

El nivel de aceptación de un VIB se establece cuando este se crea. Solo el creador del VIB puede establecer el nivel de aceptación.

Si intenta aprovisionar un host con un perfil de imagen o un VIB que tiene un nivel de aceptación más bajo que el host, se produce un error. Debe modificar el nivel de aceptación del host para instalar el perfil de imagen o el VIB. Consulte Cambiar nivel de aceptación del host. Al cambiar el nivel de aceptación del host, se modifica también su nivel de soporte.

El nivel de aceptación de un host, perfil de imagen o VIB permite determinar quién probó el VIB y quién lo admite. VMware admite los siguientes niveles de aceptación.

VMwareCertified

El nivel de aceptación VMwareCertified tiene los requisitos más estrictos. Los VIB con este nivel se someten a pruebas completamente equivalentes a las pruebas de control de calidad internas de VMware para la misma tecnología. Hoy en día, solo los controladores de los programas de proveedores de E/S (I/O Vendor Program, IOVP) se publican en este nivel. VMware responde a las llamadas de soporte para VIB con este nivel de aceptación.

VMwareAccepted

Los VIB con este nivel de aceptación pasan por pruebas de comprobación, pero estas no prueban completamente todas las funciones del software. El partner realiza pruebas y VMware comprueba el resultado. Hoy en día, los proveedores de CIM y los complementos de PSA son algunos de los VIB que se publican en este nivel. VMware dirige las llamadas de soporte para VIB con este nivel de aceptación a la organización de soporte del partner.

PartnerSupported

Los VIB con el nivel de aceptación PartnerSupported los publica un partner de confianza de VMware. El partner realiza todas las pruebas. VMware no comprueba los resultados. Este nivel se utiliza para una tecnología nueva o alternativa que los partners desean habilitar para los sistemas VMware. Hoy en día, las tecnologías de VIB de controlador, como Infiniband, ATAoE y SSD, se encuentran en este nivel con controladores de hardware que no son estándar. VMware dirige las llamadas de soporte para VIB con este nivel de aceptación a la organización de soporte del partner.

CommunitySupported

El nivel de aceptación CommunitySupported es para VIB creados por personas o empresas por fuera de los programas de partners de VMware. Los VIB de este nivel de aceptación no pasaron por un programa de pruebas aprobado por VMware y no son compatibles con el soporte técnico de VMware ni los partners de VMware.

Cambiar nivel de aceptación del host

Es posible disminuir el nivel de aceptación del host para que coincida con el de un VIB o un perfil de imagen que desea instalar.

El nivel de aceptación de cada VIB en un host debe ser por lo menos tan elevado como el nivel de aceptación del host. Por ejemplo, no es posible instalar un VIB con nivel de aceptación PartnerSupported en un host con nivel de aceptación VMwareAccepted. Primero debe disminuir el nivel de aceptación del host. Para obtener más información sobre los niveles de aceptación, consulte Niveles de aceptación.

Advertencia El cambio del nivel de aceptación del host a CommunitySupported afecta la compatibilidad del host y podría perjudicar su seguridad.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

1 Recupere el nivel de aceptación del VIB o el perfil de imagen.

Opción	Descripción
Ver información para todos los VIB	`esxcli --server=server_name software sources vib list --depot=depot_URL`
Ver información para un VIB específico	`esxcli --server=server_name software sources vib list --viburl=vib_URL`
Ver información para todos los perfiles de imagen	`esxcli --server=server_name software sources profile list --depot=depot_URL`
Ver información para un perfil de imagen específico	`esxcli --server=server_name software sources profile get --depot=depot_URL --profile=profile_name`

2 Vea el nivel de aceptación del host.

```
esxcli --server=server_name software acceptance get
```

3 Cambie el nivel de aceptación del host.

```
esxcli
             --server=server_name software acceptance set --level=acceptance_level
```

El valor de *acceptance_level* puede ser `VMwareCertified`, `VMwareAccepted`, `PartnerSupported` o `CommunitySupported`. Los valores para *acceptance_level* distinguen mayúsculas de minúsculas.

Nota Si el host tiene un nivel de aceptación más elevado que el VIB o el perfil de imagen que desea agregar, puede ejecutar comandos en el espacio de nombres `esxcli software vib` o `esxcli software profile` con la opción `--force`. Cuando utiliza la opción `--force`, aparece un mensaje de advertencia, ya que exige un VIB o un perfil de imagen con un nivel de aceptación más bajo que el del host y la configuración deja de ser coherente. La advertencia también aparece cuando instala VIB, elimina VIB o realiza ciertas otras operaciones en el host que tiene niveles de aceptación incoherentes.

Establecer el nivel de aceptación del perfil de imagen

Si desea agregar un VIB a un perfil de imagen, y el nivel de aceptación del VIB es menor al del perfil de imagen, puede clonar el perfil de imagen con un nivel de aceptación menor o cambiar el nivel de aceptación del perfil de imagen.

Puede especificar VMwareCertified, VMwareAccepted, PartnerSupported o CommunitySupported como un nivel de aceptación de un perfil de imagen. Si disminuye el nivel de aceptación, se cambiará el nivel de compatibilidad para el perfil de imagen y los hosts que aprovisiona con él. Para obtener más información, consulte Niveles de aceptación.

Requisitos previos

Instale PowerCLI y todas las herramientas de software que constituyan un requisito previo. Consulte Instalar vSphere ESXi Image Builder y software de requisito previo.

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Add-EsxSoftwareDepot` para cada almacén con el que desea trabajar.

Opción	Acción
Almacén remoto	Ejecute `Add-EsxSoftwareDepot -DepotUrl` *`depot_url`*.
Archivo ZIP	a Descargue el archivo ZIP en un sistema de archivos local. b Ejecute `Add-EsxSoftwareDepot -DepotUrl C:\file_path\`*`offline-bundle`*`.zip`.

El cmdlet devuelve uno o más objetos `SoftwareDepot`.

2 Obtenga el nivel de aceptación para el perfil de imagen.

```
Get-EsxImageProfile -Name string
```

3 Establezca el nivel de aceptación del perfil de imagen.

```
Set-EsxImageProfile -Name string -AcceptanceLevel level
```

Flujos de trabajo de vSphere ESXi Image Builder

Los flujos de trabajo de vSphere ESXi Image Builder son ejemplos del uso de cmdlets. Los flujos de trabajo no representan tareas reales, sino que ilustran cómo se pueden explorar diferentes maneras de usar un cmdlet. Los administradores que prueban los flujos de trabajo se benefician mediante una experiencia con PowerCLI, con Microsoft PowerShell o con ambos.

Revisar contenido de almacenes

Puede examinar los VIB y los almacenes de software con los cmdlets de vSphere ESXi Image Builder. Puede utilizar comodines para examinar el contenido de los almacenes. Son compatibles todas las expresiones con comodines.

El propio flujo de trabajo transmite los parámetros por nombre. No obstante, es posible acceder a variables para transmitir parámetros como objetos.

Puede utilizar opciones de filtros y expresiones con comodines para examinar el contenido de los almacenes.

Requisitos previos

Compruebe que PowerCLI y el software requerido estén instalados. Consulte Instalar vSphere ESXi Image Builder y software de requisito previo.

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Add-EsxSoftwareDepot` para cada almacén con el que desea trabajar.

Opción	Acción
Almacén remoto	Ejecute `Add-EsxSoftwareDepot -DepotUrl` *depot_url*.
Archivo ZIP	a Descargue el archivo ZIP en un sistema de archivos local. b Ejecute `Add-EsxSoftwareDepot -DepotUrl C:\file_path\`*offline-bundle*`.zip`.

El cmdlet devuelve uno o más objetos `SoftwareDepot`.

2 Recupere los perfiles de imagen.

Puede filtrarlos por proveedor, nombre y nivel de aceptación.

- ```
  Get-EsxImageProfiles
  ```

  Devuelve una matriz de objetos de `ImageProfile` provenientes de todos los almacenes que se agregaron a la sesión.

- ```
  Get-EsxImageProfile -Vendor "C*"
  ```

  Devuelve todos los perfiles de imagen creados por un proveedor cuyo nombre comienza con la letra C.

3 Recupere los paquetes de software mediante el cmdlet `Get-EsxSoftwarePackage`.

Puede filtrarlos (por ejemplo, por proveedor o versión) y puede usar los caracteres comodín estándar de PowerShell.

- ```
  Get-EsxSoftwarePackage -Vendor "V*"
  ```

  Devuelve todos los paquetes de software de un proveedor cuyo nombre comienza con la letra V.

- ```
  Get-EsxSoftwarePackage -Vendor "V*" -Name "*scsi*"
  ```

  Devuelve todos los paquetes de software cuyo nombre contiene la cadena `scsi` y que pertenecen a un proveedor cuyo nombre comienza con la letra V.

- ```
  Get-EsxSoftwarePackage -Version "2.0*"
  ```

  Devuelve todos los paquetes de software con una cadena de versión que comienza con 2.0.

4 Use `-Newest` para buscar el paquete más reciente.

- ```
  Get-EsxSoftwarePackage -Vendor "V*" -Newest
  ```

  Devuelve el paquete más reciente para los proveedores cuyo nombre comienza con la letra V y muestra la información mediante una tabla.

- ```
  Get-EsxSoftwarePackage -Vendor "V*" -Newest | format-list
  ```

  Devuelve información detallada acerca de cada paquete de software, mediante un canal que permite enlazar el resultado de la solicitud de paquetes de software emitida al cmdlet `format-list` de PowerShell.

5 Vea la lista de VIB en el perfil de imagen.

```
(Get-EsxImageProfile -Name "Robin's Profile").VibList
```

`VibList` es una propiedad del objeto `ImageProfile`.

6 Recupere los paquetes de software lanzados antes o después de una fecha determinada, mediante los parámetros `CreatedBefore` o `CreatedAfter`.

```
Get-EsxSoftwarePackage -CreatedAfter 7/1/2010
```
```

Ejemplo: Revisar el contenido de almacenes mediante variables

En este ejemplo de flujo de trabajo, se examina el contenido de un almacén mediante la transmisión de parámetros como objetos a los que se accede por posición en una variable, no mediante la transmisión de parámetros por nombre. Puede ejecutar los comandos siguientes en una secuencia desde la línea de comandos de PowerCLI. Reemplace los nombres por nombres que resulten adecuados para la instalación correspondiente.

```
Get-EsxSoftwarePackage -Vendor "V*"
Get-EsxSoftwarePackage -Vendor "V*" -Name "r*"
Get-EsxSoftwarePackage -Version "2.0*"
$ip1 = Get-EsxImageProfile -name ESX-5.0.0-123456-full
$ip1.VibList
Get-EsxSoftwarePackage -CreatedAfter 7/1/2010
```

Crear perfiles de imagen a través de un flujo de trabajo de clonación

Puede utilizar los cmdlets de vSphere ESXi Image Builder para comprobar los almacenes que están disponibles, agregar un almacén, visualizar la información de un perfil de imagen y crear un perfil de imagen nuevo mediante la clonación de uno de los perfiles de imagen disponibles.

Los perfiles publicados generalmente son de solo lectura y no pueden modificarse. Incluso si un perfil publicado no es de solo lectura, clonar en lugar de modificar el perfil es la práctica recomendada, debido a que la modificación de un perfil original elimina el original. No podrá revertir al perfil original no modificado, excepto si realiza una reconexión con un almacén.

Un flujo de trabajo de clonación de perfiles podría incluir comprobar el estado actual del sistema, agregar un almacén de software y clonar el perfil.

Requisitos previos

Compruebe que PowerCLI y el software requerido estén instalados. Consulte Instalar vSphere ESXi Image Builder y software de requisito previo.

Procedimiento

1 En una ventana de PowerShell, compruebe si se ha definido algún almacén de software para la sesión actual.

   ```
   $DefaultSoftwareDepots
   ```

   PowerShell devuelve los almacenes definidos actualmente o nada si se acaba de iniciar PowerShell.

2 Si el almacén que contiene el perfil que desea clonar no aparece en los resultados, agréguelo a la sesión actual.

Opción	Acción
Almacén remoto	Ejecute `Add-EsxSoftwareDepot -DepotUrl` *`depot_url`*.
Archivo ZIP	a Descargue el archivo ZIP en la ruta de acceso de archivo local. b Ejecute `Add-EsxSoftwareDepot -DepotUrl C:\file_path\`*`offline-bundle`*`.zip`

PowerShell agregará el almacén especificado a la sesión actual y mostrará todos los almacenes actuales.

3 (opcional) Compruebe la variable `$DefaultSoftwareDepots`, que ahora devuelve el almacén recientemente agregado.

4 Vea todos los perfiles de imagen disponibles.

```
Get-EsxImageProfile
```

5 Para clonar un perfil de imagen, introduzca su nombre, un nombre nuevo para el perfil nuevo y un nombre para el proveedor.

```
$ip = New-EsxImageProfile -CloneProfile base-tbd-v1 -Name "Test Profile 42" -Vendor
"Vendor20"
```

6 (opcional) Visualice el perfil de imagen recientemente creado, `$ip`.

PowerShell devuelve la información sobre el perfil de imagen en formato tabular.

```
Name                Vendor          Last Modified           Acceptance Level
----                ------          -------------           ----------------
Test Profile 42     Vendor20        9/15/2010 5:45:43...    PartnerSupported
```

Ejemplo: Crear un perfil de imagen mediante la clonación con variables

En este ejemplo de flujo de trabajo, se repiten los pasos de este flujo de trabajo mediante la transmisión de parámetros como objetos a los que se accede por posición en una variable, no mediante la transmisión de parámetros por nombre. Puede ejecutar los siguientes cmdlets en secuencia desde la línea de comandos de PowerCLI.

```
$DefaultSoftwareDepots
Add-EsxSoftwareDepot -DepotUrl depot_url
$DefaultSoftwareDepots
$profs = Get-EsxImageProfile
$profs
$ip = New-EsxImageProfile -CloneProfile $profs[2] -Name "new_profile_name" -Vendor "my_vendor"
$ip
```

Crear flujos de trabajo de nuevos perfiles de imagen

En la mayoría de las situaciones, se crea un perfil de imagen clonando un perfil existente. Es posible que algunos clientes o partners de VMware necesiten crear un nuevo perfil de imagen. Ponga mucha atención a las dependencias y a los niveles de aceptación en caso de que se cree un perfil de imagen desde cero.

El sistema espera que el nivel de aceptación de los VIB que se agregan a la imagen de base sea igual de alto que el nivel de la imagen de base. Si se tiene que agregar un VIB con un nivel de aceptación menor al perfil de imagen, se debe bajar el nivel de aceptación del perfil de imagen. Para obtener más información, consulte Establecer el nivel de aceptación del perfil de imagen.

Como alternativa a la especificación de los parámetros en la línea de comandos, se puede usar el mecanismo de introducción de información de PowerShell para especificar parámetros de cadena. La introducción de información no funciona para otros parámetros, como objetos.

Requisitos previos

- PowerCLI y el software de requisito previo están instalados. Consulte Instalar vSphere ESXi Image Builder y software de requisito previo.
- Tiene acceso a un almacén que incluye una imagen base y uno o más VIB. Los partners de VMware y VMware tienen almacenes públicos a los que se accede mediante URL. Los partners de VMware o VMware pueden crear un archivo ZIP que se puede descomprimir en el entorno local y al que se puede acceder mediante una ruta de acceso de archivo.

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Add-EsxSoftwareDepot` para cada almacén con el que desea trabajar.

Opción	Acción
Almacén remoto	Ejecute `Add-EsxSoftwareDepot -DepotUrl` *`depot_url`*.
Archivo ZIP	a Descargue el archivo ZIP en un sistema de archivos local. b Ejecute `Add-EsxSoftwareDepot -DepotUrl C:\file_path\`*`offline-bundle`*`.zip`.

El cmdlet devuelve uno o más objetos `SoftwareDepot`.

2 Ejecute el cmdlet `Get-EsxImageProfile` para mostrar todos los perfiles de imagen de todos los almacenes actualmente visibles. Puede limitar la búsqueda utilizando los argumentos opcionales para filtrar la salida.

```
Get-EsxSoftwarePackage -CreatedAfter 7/1/2010
```

3 Cree un nuevo perfil, asígnele un nombre y proveedor y agregue un paquete base.

```
New-EsxImageProfile -NewProfile -Name "Test #2" -vendor "Vendor42" -SoftwarePackage esx-
base[0],esx-xlibs[0]
```

El ejemplo usa el paquete esx-base. En la mayoría de los casos, cuando se crea un nuevo perfil de imagen se incluye el paquete esx-base. Los nombres que contienen espacios van con comillas.

4 Use un proceso para pasar el nuevo perfil de imagen a `format-list` para obtener información detallada sobre el nuevo paquete.

```
(Get-EsxImageProfile -Name "Test #2").VibList | format-list
```

Ejemplo: Crear perfiles de imagen desde cero utilizando variables

Esta secuencia de comandos repite los pasos del flujo de trabajo, pero pasa parámetros como objetos, a los que se accede mediante posición en una variable, en lugar de pasar parámetros por nombre. Se pueden ejecutar los siguientes comandos en secuencia en el mensaje PowerCLI.

```
Add-EsxSoftwareDepot depoturl
$pkgs = Get-EsxSoftwarePackage -CreatedAfter 7/1/2010
$ip2 = New-EsxImageProfile -NewProfile -Name "Test #2" -vendor "Vendor42" -SoftwarePackage
$pkgs[0]
$ip2.VibList | format-list
```

Editar flujo de trabajo de perfiles de imagen

Puede crear una imagen personalizada mediante la clonación y edición de un perfil de imagen utilizando PowerCLI. Puede agregar o eliminar uno o varios VIB en el perfil existente. Si agregar o eliminar VIB evita que el perfil de imagen funcione de forma correcta, se generará un error.

Requisitos previos

- PowerCLI y el software de requisito previo están instalados. Consulte Instalar vSphere ESXi Image Builder y software de requisito previo.
- Tiene acceso a un almacén que incluye una imagen base y uno o más VIB. VMware y partners de VMware permiten que estén disponibles almacenes públicos a los que se puede acceder a través de una dirección URL. VMware o partners de VMware pueden crear un archivo ZIP que puede descargar a su entorno local y acceder a través de una ruta de archivo.

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Add-EsxSoftwareDepot` para cada almacén con el que desea trabajar.

Opción	Acción
Almacén remoto	Ejecute `Add-EsxSoftwareDepot -DepotUrl` *depot_url*.
Archivo ZIP	a Descargue el archivo ZIP en un sistema de archivos local. b Ejecute `Add-EsxSoftwareDepot -DepotUrl C:\file_path\`*offline-bundle*`.zip`.

El cmdlet devuelve uno o más objetos `SoftwareDepot`.

2 Utilice una canalización para pasar el perfil de imagen que desea editar a `format-list` para acceder a información detallada.

En este ejemplo, el perfil de imagen creado en Crear flujos de trabajo de nuevos perfiles de imagen contiene solo la imagen base. No se incluye en el almacén un perfil de imagen nuevo creado. En cambio, puede acceder al perfil de imagen por el nombre o mediante la asociación con una variable.

```
Get-EsxImageProfile "Test #2" | format-list
```

PowerShell devuelve la información.

```

Name             : Test #2
Vendor            : Vendor42
...
VibList           : {esx-base 5.0.0.-...,}
```

3 (opcional) Si va a agregar un VIB con un nivel de aceptación inferior que aquel del perfil de imagen, cambie el nivel de aceptación del perfil de imagen.

```
Set-EsxImageProfile -ImageProfile "Test #2" -AcceptanceLevel VMwareAccepted
```

PowerShell devuelve la información sobre el perfil cambiado en formato tabular.

```

Name           Vendor           Last Modified       Acceptance Level
----           ------           -------------       ----------------
Test #2        Vendor42         9/22/2010 12:05:... VMwareAccepted
```

4 Agregue un paquete de software (VIB) al perfil de imagen. Puede agregar el paquete por nombre.

```
Add-EsxSoftwarePackage -ImageProfile "Test #2"
                -SoftwarePackage NewPack3
```

PowerShell devuelve la información sobre el perfil de imagen en formato tabular.

```

Name           Vendor           Last Modified       Acceptance Level
----           ------           -------------       ----------------
Test #2        Vendor42         9/22/2010 12:05:... VMwareAccepted
```

Nota Si ocurre un error cuando agrega el paquete de software, es posible que tenga un problema con los niveles de aceptación. Consulte Trabajar con niveles de aceptación

5 Vuelva a visualizar el perfil de imagen.

```
Get-EsxImageProfile "Test #2" | format-list
```

La lista de VIB se actualiza para incluir el paquete de software nuevo y se muestra la información.

```
Name             : Test #2
Vendor            : Vendor42
...
VibList           : {esx-base 5.0.0.-..., NewPack3}
```

Ejemplo: Editar perfiles de imagen a través de variables

Esta secuencia de cmdlet repite los pasos del flujo de trabajo, pero pasa los parámetros como objetos, a los que se accede a través de una posición en una variable, en lugar de pasar los parámetros por nombre. Puede ejecutar los siguientes cmdlets en secuencia desde la línea de comandos de PowerCLI.

```
Add-EsxSoftwareDepot -DepotUrl depot_url
$ip2 = Get-EsxImageProfile -name "Test #2"
$ip2 | format-list
Set-EsxImageProfile -ImageProfile $ip2 -AcceptanceLevel VMwareAccepted
Add-EsxImageSoftwarePackage -ImageProfile $ip2 -SoftwarePackage NewPack3
$ip2 | format-list
```

Información obligatoria para instalar ESXi

En una instalación interactiva, el sistema le solicita la información del sistema necesaria. En una instalación por script, debe suministrar esta información en el script de instalación.

Para su uso en el futuro, anote los valores que utilice durante la instalación. Estas anotaciones son útiles si debe reinstalar ESXi y volver a entrar los valores que eligió inicialmente.

Tabla 2-10. Información obligatoria para instalar ESXi

Información	Obligatorio u opcional	Predeterminado	Comentarios
Distribución del teclado	Obligatorio	Inglés (EE. UU.)	
identificador de VLAN	Opcional	Ninguna	Rango: de 0 a 4094
Dirección IP	Opcional	DHCP	Puede permitir que DHCP configure la red durante la instalación. Después de la instalación, puede cambiar la configuración de red.
Máscara de subred	Opcional	Se calcula en base a la dirección IP	
Puerta de enlace	Opcional	En función de la dirección IP y la máscara de subred configuradas	
DNS principal	Opcional	En función de la dirección IP y la máscara de subred configuradas	
DNS secundario	Opcional	Ninguna	

Tabla 2-10. Información obligatoria para instalar ESXi (continuación)

Información	Obligatorio u opcional	Predeterminado	Comentarios
Nombre de host	Obligatorio para la configuración de IP estática	Ninguna	vSphere Web Client puede utilizar el nombre de host o la dirección IP para acceder al host ESXi.
Ubicación de instalación	Obligatorio	Ninguna	Debe tener al menos 5 GB si va a instalar los componentes en un único disco.
Migrar la configuración de ESXi existente. Conservar el almacén de datos de VMFS existente.	Obligatorio si va a instalar ESXi en una unidad con una instalación de ESXi existente.	Ninguna	Si ya existe una instalación de ESXi 5.x, el instalador de ESXi permite elegir entre conservar o sobrescribir el almacén de datos de VMFS durante la instalación
Contraseña raíz	Obligatorio	Ninguna	La contraseña raíz debe contener entre 8 y 40 caracteres. Para obtener información sobre las contraseñas, consulte la documentación sobre la *seguridad de vSphere*.

Instalación de ESXi

Puede instalar ESXi de forma interactiva, con una instalación generada por script o con vSphere Auto Deploy.

Instalar ESXi de forma interactiva

Utilice la opción de instalación interactiva para implementaciones pequeñas con menos de cinco hosts.

En una instalación interactiva típica, debe arrancar el instalador de ESXi y responder las solicitudes para instalar ESXi en el disco host local. El instalador vuelve a formatear y particiona el disco de destino y, a continuación, instala la imagen de arranque de ESXi. Si no instaló ESXi en el disco de destino antes, se sobrescribirán todos los datos de la unidad. Esto incluye las particiones de proveedores de hardware, las particiones de sistemas operativos y los datos asociados.

Nota Para asegurarse de no perder datos, mígrelos a otro equipo antes de instalar ESXi.

Si va a instalar ESXi en un disco que contiene una instalación anterior de ESXi o ESX, o bien un almacén de datos de VMFS, el instalador le brindará opciones para actualización. Consulte la documentación sobre la *actualización de vSphere*.

Instalar ESXi de forma interactiva

Utilice el CD/DVD o una unidad flash USB de ESXi para instalar el software ESXi en un disco duro SAS, SATA o SCSI, o bien en una unidad USB.

Requisitos previos

- Debe tener el archivo ISO del instalador de ESXi en una de las siguientes ubicaciones:
  - Un CD o DVD. Si no posee el CD/DVD de instalación, puede crear uno. Consulte Descargar y grabar un CD or DVD de la imagen ISO del instalador de ESXi
  - Una unidad flash USB. Consulte Formatear una unidad flash USB para arrancar la instalación o la actualización de ESXi.

Nota También puede realizar un arranque PXE del instalador de ESXi para ejecutar una instalación interactiva o por script. Consulte Arranque PXE del instalador de ESXi.

- Compruebe que el reloj de hardware del servidor esté configurado como UTC. Esta configuración se encuentra en el BIOS del sistema.
- Compruebe que haya un teclado y un monitor conectados al equipo en el que está instalado el software ESXi. Como alternativa, utilice una aplicación de administración remota. Consulte Usar aplicaciones de administración remota.
- Considere la posibilidad de desconectar el almacenamiento de red. Esta acción disminuye el tiempo que tarda el instalador en buscar unidades de disco disponibles. Al desconectar el almacenamiento de red, ninguno de los archivos almacenados en los discos desconectados está disponible durante la instalación.

  No desconecte un LUN que contenga una instalación de ESX o ESXi. No desconecte un almacén de datos de VMFS que contenga una consola de servicios de una instalación de ESX existente. Estas acciones podrían afectar el resultado de la instalación.
- Recopile la información que necesita el asistente de instalación de ESXi. Consulte Información obligatoria para instalar ESXi.
- La contraseña raíz debe contener entre 8 y 40 caracteres. De manera predeterminada, cuando cree la contraseña deberá incluir una combinación de cuatro clases de caracteres: letras en minúscula, letras en mayúscula, números y caracteres especiales, como el guion bajo o el guion. Para obtener información sobre las contraseñas de ESXi, consulte "Bloqueo de cuenta y contraseñas ESXi" en la documentación de *Seguridad de vSphere*.
- Compruebe que ESXi Embedded no esté presente en el equipo host. ESXi Installable y ESXi Embedded no pueden estar en el mismo host.

Procedimiento

1. Inserte el CD/DVD del instalador de ESXi en la unidad de CD/DVD-ROM, o bien conecte la unidad flash USB del instalador, y reinicie el equipo.
2. Configure el BIOS para que arranque desde el dispositivo de CD-ROM o la unidad flash USB.

   Consulte la documentación del proveedor de hardware para obtener información sobre el cambio del orden de arranque.

3 En la página Seleccionar un disco, seleccione la unidad en la que va a instalar ESXi y presione Entrar.

Presione F1 para obtener más información sobre el disco seleccionado.

Nota No se base en el orden de discos de la lista para seleccionar un disco. El BIOS determina el orden de discos y podría estar desordenado. Esto puede ocurrir en sistemas en los que se agregan y eliminan unidades continuamente.

Si selecciona un disco que contiene datos, aparece la página Confirmar selección de disco.

Si va a realizar la instalación en un disco que tiene una instalación anterior de ESXi o ESX, o bien en un almacén de datos de VMFS, el instalador proporciona varias alternativas.

Importante Si va a actualizar o migrar una instalación de ESX/ESXi existente, consulte la documentación sobre *Actualizar vSphere*. Las instrucciones de la documentación sobre *Instalar y configurar vSphere* son para una instalación nueva de ESXi nueva.

Si selecciona un disco del grupo de discos de vSAN, la instalación que se obtenga dependerá del tipo de disco y del tamaño del grupo:

- Si selecciona una SSD, esta y todas las HDD subyacentes del mismo grupo de discos se borrarán.
- Si selecciona una HDD y el tamaño del grupo de discos es mayor que 2, solo se borrará la HDD seleccionada.
- Si selecciona una HDD y el tamaño del grupo de discos es 2 o menos, se borrarán la SSD y la HDD seleccionada.

Para obtener más información acerca de la administración de grupos de discos de vSAN, consulte la documentación de *Almacenamiento de vSphere*.

4 Seleccione el tipo de teclado para el host.

Después de la instalación, puede cambiar el tipo de teclado en la consola directa.

5 Escriba la contraseña raíz para el host.

Después de la instalación, puede cambiar la contraseña en la consola directa.

6 Presione Intro para iniciar la instalación.

7 Una vez que esta finaliza, quite el CD, el DVD o la unidad flash USB de instalación.

8 Presione Intro para reiniciar el host.

Cuando realiza una nueva instalación o decide sobrescribir un almacén de datos de VMFS existente, durante la operación de reinicio, se crean particiones VFAT desde cero y VMFS en el disco host.

9 Configure el dispositivo de primer arranque como la unidad en la que instaló ESXi en Paso 3.

   Para obtener más información sobre cómo cambiar el orden de arranque, consulte la documentación del proveedor de hardware.

   Nota Es posible que se necesiten pasos adicionales para configurar el dispositivo de arranque en sistemas UEFI. Consulte El host no arranca después de instalar ESXi en modo UEFI

Resultados

Una vez finalizada la instalación, puede migrar los datos de VMFS existentes al host ESXi.

Puede arrancar un único equipo desde cada imagen de ESXi. No se permite arrancar varios dispositivos desde una única imagen compartida de ESXi.

Pasos siguientes

Establezca la configuración básica de administración y red para ESXi. Consulte Después de instalar y configurar ESXi.

Instalar ESXi en un disco iSCSI de software

Al instalar ESXi en un disco iSCSI de software, debe configurar el nombre calificado iSCSI (IQN) de destino.

Durante el arranque del sistema, se realiza una prueba automática de encendido (POST) y se comienzan a iniciar los adaptadores en el orden especificado en el BIOS del sistema. Cuando el orden de arranque llega al adaptador de la tabla de firmware de arranque de iSCSI (iBFT), el adaptador intenta conectarse al destino, pero no arranca desde el destino. Consulte los requisitos previos.

Si la conexión con el destino de iSCSI se establece correctamente, el firmware de arranque de iSCSI guarda la configuración de arranque de iSCSI en iBFT. El próximo adaptador en arrancar debe ser el medio de instalación de ESXi, que puede ser una imagen ISO montada o un CD-ROM físico.

Requisitos previos

- Compruebe que el IQN de destino esté establecido en la configuración de parámetros de destino del BIOS de iBFT. Esta configuración se encuentra en la opción ROM de la tarjeta de interfaz de red (NIC) que se debe usar para el LUN de iSCSI. Consulte la documentación del proveedor de su sistema.
- Deshabilite la opción del adaptador de iBFT para arrancar en el destino de iSCSI. Esta acción es necesaria para garantizar el arranque del instalador de ESXi, en lugar del destino de iSCSI. Al iniciar el sistema, siga el aviso para iniciar sesión en el adaptador de iBFT y deshabilite la opción para arrancar en el destino de iSCSI. Consulte la documentación del proveedor de su sistema y su adaptador de iBFT. Después de finalizar la instalación de ESXi, puede volver a habilitar la opción para arrancar desde el LUN en el que instaló ESXi.

Procedimiento

1 Inicie la instalación interactiva desde la imagen ISO montada o el CD/DVD de instalación de ESXi.

2 En la pantalla Seleccionar un disco, seleccione el destino de iSCSI que especificó en la configuración de parámetros de destino del BIOS de iBFT.

   Si el destino no aparece en este menú, asegúrese de que la configuración de TCP/IP e IQN iSCSI del iniciador sea la correcta. Compruebe la lista de control de acceso (ACL) de la red y confirme que el adaptador cuenta con los permisos necesarios para acceder al destino.

3 Siga las indicaciones para completar la instalación.

4 Reinicie el host.

5 En la configuración del BIOS del host, especifique la configuración del BIOS para el adaptador de iBFT y cambie el parámetro del adaptador para que arranque desde el destino de iSCSI.

   Consulte la documentación del proveedor de su sistema.

Pasos siguientes

En el adaptador de iBFT, habilite nuevamente la opción para arrancar en el destino de iSCSI, de modo que el sistema arranque desde el LUN en el que instaló ESXi.

Instalar o actualizar hosts mediante un script

Puede implementar hosts de ESXi rápidamente mediante instalaciones o actualizaciones desatendidas generadas por script. Las instalaciones o las actualizaciones generadas por script proporcionan un mecanismo eficaz para la implementación de varios hosts.

El script de instalación o actualización contiene la configuración de instalación para ESXi. Puede aplicar el script a todos los que desee que tengan una configuración similar.

Para una instalación o una actualización generada por script, debe usar los comandos compatibles para crear un script. Puede editar el script con la finalidad de cambiar ajustes de configuración que sean exclusivos para cada host.

El script de instalación o actualización puede residir en una de las ubicaciones siguientes:

- Servidor FTP
- Servidor HTTP/HTTPS
- servidor NFS
- Unidad flash USB
- Unidad de CD-ROM

Enfoques para la instalación por script

Puede instalar ESXi en varios equipos con un único script para todos o un script separado para cada uno.

Por ejemplo, debido a que los nombres de disco varían de un equipo a otro, una de las opciones de configuración que se recomienda seleccionar en un script es el disco en el que se va a instalar ESXi.

Tabla 2-11. Opciones de una instalación por script

Opción	Acción
Instalar siempre en el primer disco de varios equipos.	Crear un solo script.
Instalar ESXi en un disco distinto para cada equipo.	Crear varios scripts.

Para obtener información sobre los comandos necesarios para especificar el disco en el que se va a realizar la instalación, consulte Comandos de scripts de instalación y actualización.

Introducir las opciones de arranque para iniciar un script de instalación o actualización

Puede iniciar un script de instalación o actualización introduciendo las opciones de arranque en la línea de comandos de arranque del instalador de ESXi.

En el momento del arranque, es posible que necesite especificar opciones para acceder al archivo de inicio. Puede introducir opciones de arranque presionando Shift+O en el gestor de arranque. Para una instalación de arranque PXE, puede pasar opciones a través de la línea `kernelopts` del archivo `boot.cfg`. Consulte Acerca del archivo boot.cfg y Arranque PXE del instalador de ESXi.

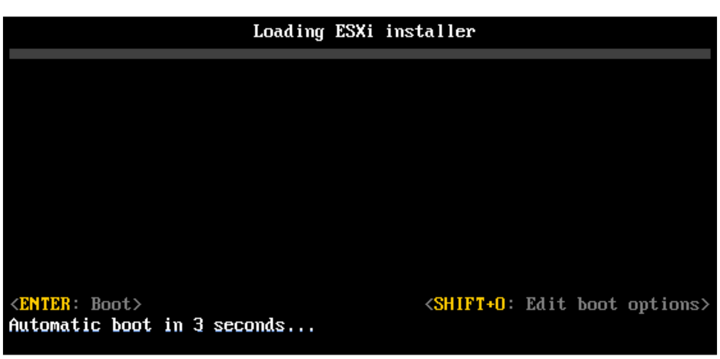
Para especificar la ubicación del script de instalación, defina la opción `ks=`*`filepath`*, donde *filepath* indica la ubicación del archivo Kickstart. De lo contrario, no se podrá iniciar una instalación o actualización generadas por script. Si se omite `ks=`*`filepath`*, se ejecuta el instalador de texto.

Las opciones de arranque compatibles se detallan en Opciones de arranque .

Procedimiento

1 Inicie el host.

2 Cuando aparezca la ventana del instalador de ESXi, presione las teclas Mayús + O para editar las opciones de arranque.



3 En el símbolo del sistema `runweasel`, introduzca **`ks=`*`ubicación del script de instalación más las opciones de la línea de comandos de arranque`***.

Ejemplo: Opción de arranque

Introduzca las siguientes opciones de arranque:

```
ks=http://00.00.00.00/kickstart/ks-osdc-pdp101.cfg nameserver=00.00.0.0 ip=00.00.00.000
netmask=255.255.255.0 gateway=00.00.00.000
```

Opciones de arranque

Cuando realice una instalación por script, es posible que necesite especificar opciones en el arranque para acceder al archivo de inicio.

Opciones de arranque compatibles

Tabla 2-12. Opciones de arranque para la instalación de ESXi

Opción de arranque	Descripción
`BOOTIF=`*`hwtype-MAC address`*	Similar a la opción `netdevice`, excepto en el formato PXELINUX, tal como se describe en la opción IPAPPEND en SYSLINUX en el sitio syslinux.zytor.com.
`gateway=`*`ip address`*	Permite establecer esta puerta de enlace de red como la puerta de enlace predeterminada para utilizarla en la descarga de scripts de instalación y medios de instalación.
`ip=`*`ip address`*	Permite configurar una dirección IP estática para utilizarla en la descarga de scripts de instalación y medios de instalación. Nota: también se admite el formato PXELINUX para esta opción. Consulte la opción IPAPPEND en SYSLINUX en el sitio syslinux.zytor.com.
`ks=cdrom:/`*`path`*	Permite realizar una instalación por script con el script en *path*, que se encuentra en el CD de la unidad de CD-ROM. Cada CDROM se monta y se comprueba hasta que se encuentre el archivo que coincida con la ruta de acceso. **Importante** Si creó una imagen ISO de instalador con un script de instalación o actualización personalizado, debe utilizar caracteres en mayúscula para proporcionar la ruta de acceso del script, por ejemplo, `ks=cdrom:/KS_CUST.CFG`.
`ks=file://`*`path`*	Realiza una instalación por script con el script en *path*.
`ks=`*`protocol`*`://`*`serverpath`*	Realiza una instalación por script con un script ubicado en la red en la dirección URL determinada. *protocol* puede ser `http`, `https`, `ftp` o `nfs`. Un ejemplo de uso del protocolo nfs es `ks=nfs://`*`host/porturl-path`*. El formato de la URL de NFS se especifica en RFC 2224.
`ks=usb`	Realiza una instalación por script mediante el acceso al script desde la unidad USB conectada. Busca un archivo con el nombre `ks.cfg`. El archivo debe estar ubicado en el directorio raíz de la unidad. Si se conectan varias unidades flash USB, se realizará la búsqueda hasta que se encuentre el archivo `ks.cfg`. Solo se admiten los sistemas de archivos FAT16 y FAT32.

Tabla 2-12. Opciones de arranque para la instalación de ESXi (continuación)

Opción de arranque	Descripción
`ks=usb:/`*`path`*	Realiza una instalación por script con un archivo de script en la ruta especificada, que se encuentra en USB.
`ksdevice=`*`device`*	Intenta utilizar un adaptador de red *device* cuando se realiza la búsqueda de un script de instalación y un medio de instalación. Se especifica como una dirección MAC, por ejemplo, 00:50:56:C0:00:01. Esta ubicación también puede ser un nombre vmnicNN. Si no se especifica y los archivos deben obtenerse a través de la red, el instalador utiliza de forma predeterminada el primer adaptador de red detectado que esté conectado.
`nameserver=`*`ip address`*	Especifica un servidor de nombres de dominio para utilizarlo en la descarga de scripts de instalación y medios de instalación.
`netdevice=`*`device`*	Intenta utilizar un adaptador de red *device* cuando se realiza la búsqueda de un script de instalación y un medio de instalación. Se especifica como una dirección MAC, por ejemplo, 00:50:56:C0:00:01. Esta ubicación también puede ser un nombre vmnicNN. Si no se especifica y los archivos deben obtenerse a través de la red, el instalador utiliza de forma predeterminada el primer adaptador de red detectado que esté conectado.
`netmask=`*`subnet mask`*	Especifica una máscara de subred para la interfaz de red que descarga los scripts de instalación y los medios de instalación.
`vlanid=`*`vlanid`*	Configure la tarjeta de red para que se encuentre en la VLAN especificada.

Acerca de los scripts de instalación y actualización

El script de instalación o actualización es un archivo de texto que contiene los comandos compatibles (por ejemplo, `ks.cfg`).

La sección de comandos del script contiene las opciones de instalación de ESXi. Esta sección es obligatoria y debe aparecer primero en el script.

Acerca del script de instalación predeterminado ks.cfg

El instalador de ESXi incluye un script de instalación predeterminado que realiza una instalación estándar en el primer disco detectado.

El script de instalación `ks.cfg` predeterminado está ubicado en el disco RAM inicial en `/etc/vmware/weasel/ks.cfg`. Puede especificar la ubicación del archivo `ks.cfg` predeterminado con la opción de arranque `ks=file://etc/vmware/weasel/ks.cfg`. Consulte Introducir las opciones de arranque para iniciar un script de instalación o actualización.

Cuando instale ESXi con el script `ks.cfg`, la contraseña raíz predeterminada será `mypassword`.

No puede modificar el script predeterminado en los medios de instalación. Después de la instalación, puede utilizar vSphere Web Client para iniciar sesión en vCenter Server que administra el host ESXi y modificar la configuración predeterminada.

El script predeterminado contiene los siguientes comandos:

```
#
# Sample scripted installation file
#

# Accept the VMware End User License Agreement
vmaccepteula

# Set the root password for the DCUI and Tech Support Mode
rootpw mypassword

# Install on the first local disk available on machine
install --firstdisk --overwritevmfs

# Set the network to DHCP on the first network adapter
network --bootproto=dhcp --device=vmnic0

# A sample post-install script
%post --interpreter=python --ignorefailure=true
import time
stampFile = open('/finished.stamp', mode='w')
stampFile.write( time.asctime() )
```

Ubicaciones admitidas para scripts de instalación o actualización

En instalaciones y actualizaciones generadas por script, el instalador de ESXi puede acceder al script de la instalación o actualización, que también se conoce como el archivo inicial, desde varias ubicaciones.

Se admiten las siguientes ubicaciones para el script de instalación o actualización:

- CD/DVD. Consulte Crear una imagen ISO de instalador con un script de instalación o actualización personalizado.
- Unidad flash USB. Consulte Crear una unidad flash USB para almacenar el script de instalación o actualización de ESXi.
- Una ubicación local de red a la que se puede acceder mediante los siguientes protocolos: NFS, HTTP, HTTPS, FTP

Ruta de acceso del script de instalación o actualización

Puede especificar la ruta de acceso de un script de instalación o actualización.

`ks=http://`*`XXX.XXX.XXX.XXX`*`/kickstart/KS.CFG` es la ruta de acceso del script de instalación de ESXi, donde*`XXX.XXX.XXX.XXX`*es la dirección IP del equipo donde reside el script. Consulte Acerca de los scripts de instalación y actualización.

Para iniciar un script de instalación desde una instalación interactiva, escriba la opción `ks=` de forma manual. Consulte Introducir las opciones de arranque para iniciar un script de instalación o actualización.

Comandos de scripts de instalación y actualización

Para modificar el script predeterminado de instalación o actualización, o para crear su propio script, use comandos compatibles. Use comandos compatibles en el script de instalación, que se especifica mediante un comando de arranque cuando se arranca el instalador.

Para determinar en qué disco instalar o actualizar ESXi, el script de instalación requiere uno de los comandos siguientes: `install`, `upgrade` o `installorupgrade`. El comando `install` crea las particiones predeterminadas, que incluyen un almacén de datos de VMFS que ocupa todo el espacio disponible después de que se crean las demás particiones.

accepteula o vmaccepteula (obligatorio)

Acepta el contrato de licencia de ESXi.

clearpart (opcional)

Borra las particiones existentes del disco. Requiere que se especifique el comando `install`. Edite cuidadosamente el comando `clearpart` en sus scripts existentes.

`--drives=`
Quita las particiones en las unidades especificadas.

`--alldrives`
Ignora el requisito de `--drives=` y permite borrar las particiones de cada unidad.

`--ignoredrives=`
Elimina las particiones en todas las unidades, excepto las especificadas. Es obligatorio a menos que se especifiquen las marcas `--drives=` o `--alldrives`.

`--overwritevmfs`
Permite sobrescribir las particiones de VMFS en las unidades especificadas. De forma predeterminada, no se permite sobrescribir las particiones de VMFS.

`--firstdisk=` ***`tipo-disco1`*** **`[`*`tipo-disco2`*`,...]`**
Particiona el primer disco encontrado que satisface las condiciones. De forma predeterminada, los discos que satisfacen las condiciones se ordenan en el orden siguiente:

1 Almacenamiento conectado a nivel local (`local`)

2 Almacenamiento en red (`remote`)

3 Discos USB (`usb`)

Puede cambiar el orden de los discos anexando una lista separada por comas al argumento. Si proporciona una lista de filtros, se sobrescribe la configuración predeterminada. Puede combinar filtros para especificar un disco en particular, lo que incluye `esx` para el primer disco en el que se haya instalado ESXi, la información de

modelo y proveedor, o el nombre del controlador del dispositivo VMkernel. Por ejemplo, para dar preferencia a un disco con el nombre de modelo ST3120814A y a cualquier disco que use el controlador mptsas en lugar de un disco local normal, el argumento es `--firstdisk=ST3120814A,mptsas,local`. Puede utilizar `localesx` para el almacenamiento local que contiene la imagen de ESXi o `remoteesx` para el almacenamiento remoto que contiene la imagen deESXi.

dryrun (opcional)

Analiza y comprueba el script de instalación. No ejecuta la instalación.

instalar

Especifica que se trata de una instalación nueva. Reemplaza el comando `autopart` obsoleto que se utilizaba para las instalaciones generadas por script de ESXi 4.1. Se requieren los comandos `install`, `upgrade` o `installorupgrade` para determinar en qué disco se debe instalar o actualizar ESXi.

`--disk= or --drive=`

Especifica el disco que se particionará. En el comando `--disk=`*`diskname`*, el valor *diskname* puede tener cualquiera de los formatos que se muestran en los ejemplos siguientes:

- Ruta de acceso: `--disk=`*`/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`*
- Nombre de MPX: `--disk=`*`mpx.vmhba1:C0:T0:L0`*
- Nombre de VML: `--disk=`*`vml.000000034211234`*
- UID de vmkLUN: `--disk=`*`vmkLUN_UID`*

Para conocer los formatos admitidos de nombre de disco, consulte Nombre de los dispositivos de disco.

`--firstdisk=`
`tipo-disco1,`
`[`*`tipo-disco2`*`,...]`

Particiona el primer disco encontrado que satisface las condiciones. De forma predeterminada, los discos que satisfacen las condiciones se ordenan en el orden siguiente:

1. Almacenamiento conectado a nivel local (`local`)
2. Almacenamiento en red (`remote`)
3. Discos USB (`usb`)

Puede cambiar el orden de los discos anexando una lista separada por comas al argumento. Si proporciona una lista de filtros, se sobrescribe la configuración predeterminada. Puede combinar filtros para especificar un disco en particular, lo que incluye `esx` para el primer disco en el que se haya instalado ESX, la información de modelo y proveedor, o el nombre del controlador del dispositivo

	VMkernel. Por ejemplo, para dar preferencia a un disco con el nombre de modelo ST3120814A y a cualquier disco que use el controlador mptsas en lugar de un disco local normal, el argumento es `--firstdisk=ST3120814A,mptsas,local`. Puede utilizar `localesx` para el almacenamiento local que contiene la imagen de ESXi o `remoteesx` para el almacenamiento remoto que contiene la imagen deESXi.
`--ignoressd`	Excluye los discos de estado sólido de los que satisfacen las condiciones para el particionamiento. Esta opción puede utilizarse con el comando `install` y la opción `--firstdisk`. Esta opción tiene prioridad sobre la opción `--firstdisk`. Esta opción no es válida con las opciones `--drive` o `--disk` ni con los comandos `upgrade` o `installorupgrade`. Consulte la documentación de *Almacenamiento de vSphere* para obtener más información sobre la prevención del formateo de SSD durante la creación automática de particiones.
`--overwritevsan`	Debe usar la opción `--overwritevsan` cuando instale ESXi en un disco, ya sea SSD o HDD (magnética), que forme parte de un grupo de discos de vSAN. Si usa esta opción y no hay ninguna partición de vSAN en el disco seleccionado, se produce un error en la instalación. Al instalar ESXi en un disco que forma parte de un grupo de discos de vSAN, el resultado depende del disco que se selecciona: ▪ Si selecciona una SSD, esta y todas las HDD subyacentes del mismo grupo de discos se borrarán. ▪ Si selecciona una HDD, y el tamaño del grupo de discos es mayor que 2, solo se borrarán las HDD seleccionadas. ▪ Si selecciona una HDD y el tamaño del grupo de discos es 2 o menos, se borrarán la SSD y las HDD seleccionadas. Para obtener más información acerca de la administración de grupos de discos de vSAN, consulte la documentación de *Almacenamiento de vSphere*.
`--overwritevmfs`	Es obligatorio para sobrescribir un almacén de datos existente de VMFS en el disco antes de la instalación.
`--preservevmfs`	Conserva el almacén de datos existente de VMFS en el disco durante la instalación.
`--novmfsondisk`	Impide que se cree una partición de VMFS en este disco. Debe utilizarse con `--overwritevmfs` si ya existe una partición de VMFS en el disco.

installorupgrade

Se requieren los comandos `install`, `upgrade` o `installorupgrade` para determinar en qué disco se debe instalar o actualizar ESXi.

`--disk= or --drive=`

Especifica el disco que se particionará. En el comando `--disk=`*`diskname`*, el valor *diskname* puede tener cualquiera de los formatos que se muestran en los ejemplos siguientes:

- Ruta de acceso: `--disk=`*`/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`*
- Nombre de MPX: `--disk=`*`mpx.vmhba1:C0:T0:L0`*
- Nombre de VML: `--disk=`*`vml.000000034211234`*
- UID de vmkLUN: `--disk=`*`vmkLUN_UID`*

Para conocer los formatos admitidos de nombre de disco, consulte Nombre de los dispositivos de disco.

`--firstdisk=` ***`tipo-disco1,`*** **`[`*`tipo-disco2`*`,...]`**

Particiona el primer disco encontrado que satisface las condiciones. De forma predeterminada, los discos que satisfacen las condiciones se ordenan en el orden siguiente:

1. Almacenamiento conectado a nivel local (`local`)
2. Almacenamiento en red (`remote`)
3. Discos USB (`usb`)

Puede cambiar el orden de los discos anexando una lista separada por comas al argumento. Si proporciona una lista de filtros, se sobrescribe la configuración predeterminada. Puede combinar filtros para especificar un disco en particular, lo que incluye `esx` para el primer disco en el que se haya instalado ESX, la información de modelo y proveedor, o el nombre del controlador del dispositivo VMkernel. Por ejemplo, para dar preferencia a un disco con el nombre de modelo ST3120814A y a cualquier disco que use el controlador mptsas en lugar de un disco local normal, el argumento es `--firstdisk=ST3120814A,mptsas,local`. Puede utilizar `localesx` para el almacenamiento local que contiene la imagen de ESXi o `remoteesx` para el almacenamiento remoto que contiene la imagen deESXi.

`--overwritevsan`

Debe usar la opción `--overwritevsan` cuando instale ESXi en un disco, ya sea SSD o HDD (magnética), que forme parte de un grupo de discos de vSAN. Si usa esta opción y no hay ninguna partición de vSAN en el disco seleccionado, se produce un error en la instalación.

	Al instalar ESXi en un disco que forma parte de un grupo de discos de vSAN, el resultado depende del disco que se selecciona: ■ Si selecciona una SSD, esta y todas las HDD subyacentes del mismo grupo de discos se borrarán. ■ Si selecciona una HDD, y el tamaño del grupo de discos es mayor que 2, solo se borrarán las HDD seleccionadas. ■ Si selecciona una HDD y el tamaño del grupo de discos es 2 o menos, se borrarán la SSD y las HDD seleccionadas. Para obtener más información acerca de la administración de grupos de discos de vSAN, consulte la documentación de *Almacenamiento de vSphere*.
`--overwritevmfs`	Instale ESXi si en el disco existe una partición de VMFS, pero no una instalación de ESX ni ESXi. A menos que esta opción esté presente, se producirá un error en el instalador si en el disco existe una partición de VMFS, pero no una instalación de ESX ni ESXi.

keyboard (opcional)

Configura el tipo de teclado para el sistema.

`keyboardType`	Especifica la distribución del teclado para el tipo de teclado seleccionado. El parámetro *keyboardType* debe ser de uno de los tipos siguientes. ■ Belgian ■ Brazilian ■ Croatian ■ Czechoslovakian ■ Danish ■ Estonian ■ Finnish ■ Francés ■ Alemán ■ Greek ■ Icelandic ■ Italian ■ Japonés ■ Latin American

- Norwegian
- Polish
- Portuguese
- Russian
- Slovenian
- Español
- Swedish
- Swiss French
- Swiss German
- Turkish
- Ukrainian
- United Kingdom
- Inglés americano (predeterminado)
- US Dvorak

serialnum o vmserialnum (opcional)

Obsoletos en ESXi 5.0.x. Compatibles con ESXi 5.1 y versiones superiores. Configura las licencias. Si no se incluye, ESXi se instala en modo de evaluación.

`--esx=<license-key>`	Especifica la clave de licencia de vSphere que se utilizará. El formato corresponde a cinco grupos de cinco caracteres (XXXXX-XXXXX-XXXXX-XXXXX-XXXXX).

network (opcional)

Especifica una dirección de red para el sistema.

`--bootproto=[dhcp|static]`	Especifica si la configuración de red se debe obtener desde DHCP o si se debe configurar de forma manual.
`--device=`	Especifica la dirección MAC de la tarjeta de red o el nombre del dispositivo, con el formato `vmnicNN` (por ejemplo, `vmnic0`). Esta opción hace referencia al dispositivo del vínculo superior para el conmutador virtual.
`--ip=`	Establece una dirección IP para el equipo que se va a instalar, con el formato `xxx.xxx.xxx.xxx`. Es obligatorio cuando se usa la opción `--bootproto=static` y se ignora en los demás casos.

--gateway=	Designa la puerta de enlace predeterminada como una dirección IP, con el formato `xxx.xxx.xxx.xxx`. Se usa con la opción `--bootproto=static`.
--nameserver=	Designa el servidor de nombre principal como una dirección IP. Se usa con la opción `--bootproto=static`. Omita esta opción si no va a usar DNS. La opción `--nameserver` puede admitir dos direcciones IP. Por ejemplo: `--nameserver="10.126.87.104[,10.126.87.120]"`
--netmask=	Especifica la máscara de subred para el sistema instalado, con el formato `255.xxx.xxx.xxx`. Se usa con la opción `--bootproto=static`.
--hostname=	Especifica el nombre de host para el sistema instalado.
--vlanid= ***vlanid***	Especifica la VLAN en la que reside el sistema. Se usa con las opciones `--bootproto=dhcp` o `--bootproto=static`. Se establece como un valor entero entre 1 y 4096.
--addvmportgroup=(0|1)	Especifica si se debe agregar el grupo de puertos de la red de máquinas virtuales (VM), que utilizan las máquinas virtuales. El valor predeterminado es 1.

paranoid (opcional)

Hace que los mensajes de advertencia interrumpan la instalación. Si omite este comando, los mensajes de advertencia se registran.

part o partition (opcional)

Crea un almacén de datos de VMFS en el sistema. Solo se puede crear un almacén de datos por cada disco. No se puede usar en el mismo disco que el comando `install`. Solo se puede especificar una partición por cada disco y solo puede ser una partición de VMFS.

datastore name	Especifica dónde se debe montar la partición.
--ondisk= or --ondrive=	Especifica el disco o la unidad en la que se crea la partición.
--firstdisk= ***tipo-disco1*, ** **[*tipo-disco2*,...]**	Particiona el primer disco encontrado que satisface las condiciones. De forma predeterminada, los discos que satisfacen las condiciones se ordenan en el orden siguiente: 1 Almacenamiento conectado a nivel local (`local`) 2 Almacenamiento en red (`remote`) 3 Discos USB (`usb`)

Puede cambiar el orden de los discos anexando una lista separada por comas al argumento. Si proporciona una lista de filtros, se sobrescribe la configuración predeterminada. Puede combinar filtros para especificar un disco en particular, lo que incluye `esx` para el primer disco en el que se haya instalado ESX, la información de modelo y proveedor, o el nombre del controlador del dispositivo VMkernel. Por ejemplo, para dar preferencia a un disco con el nombre de modelo ST3120814A y a cualquier disco que use el controlador mptsas en lugar de un disco local normal, el argumento es `--firstdisk=ST3120814A,mptsas,local`. Puede utilizar `localesx` para el almacenamiento local que contiene la imagen de ESXi o `remoteesx` para el almacenamiento remoto que contiene la imagen deESXi.

reboot (opcional)

Reinicia la máquina después de que finaliza la instalación generada por script.

<--noeject>	No se expulsa el CD después de la instalación.

rootpw (obligatorio)

Configura la contraseña raíz para el sistema.

--iscrypted	Especifica que la contraseña está cifrada.
password	Especifica el valor de la contraseña.

actualizar

Se requieren los comandos `install`, `upgrade` o `installorupgrade` para determinar en qué disco se debe instalar o actualizar ESXi.

--disk= or --drive=

Especifica el disco que se particionará. En el comando `--disk=`*`diskname`*, el valor *diskname* puede tener cualquiera de los formatos que se muestran en los ejemplos siguientes:

- Ruta de acceso: `--disk=`*`/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`*
- Nombre de MPX: `--disk=`*`mpx.vmhba1:C0:T0:L0`*
- Nombre de VML: `--disk=`*`vml.000000034211234`*
- UID de vmkLUN:`--disk=`*`vmkLUN_UID`*

	Para conocer los formatos admitidos de nombre de disco, consulte Nombre de los dispositivos de disco.
--firstdisk= ***tipo-disco1,*** **[*tipo-disco2*,...]**	Particiona el primer disco encontrado que satisface las condiciones. De forma predeterminada, los discos que satisfacen las condiciones se ordenan en el orden siguiente: 1 Almacenamiento conectado a nivel local (`local`) 2 Almacenamiento en red (`remote`) 3 Discos USB (`usb`) Puede cambiar el orden de los discos anexando una lista separada por comas al argumento. Si proporciona una lista de filtros, se sobrescribe la configuración predeterminada. Puede combinar filtros para especificar un disco en particular, lo que incluye `esx` para el primer disco en el que se haya instalado ESX, la información de modelo y proveedor, o el nombre del controlador del dispositivo VMkernel. Por ejemplo, para dar preferencia a un disco con el nombre de modelo ST3120814A y a cualquier disco que use el controlador mptsas en lugar de un disco local normal, el argumento es `--firstdisk=ST3120814A,mptsas,local`. Puede utilizar `localesx` para el almacenamiento local que contiene la imagen de ESXi o `remoteesx` para el almacenamiento remoto que contiene la imagen deESXi.

%include o include (opcional)

Especifica otro script de instalación para analizar. Este comando se utiliza de manera similar a un comando de varias líneas, pero usa solamente un argumento.

filename	Por ejemplo: `%include part.cfg`

%pre (opcional)

Especifica un script para ejecutar antes de que se evalúe la configuración de inicio. Por ejemplo, puede usarse para generar los archivos que incluirá el archivo de inicio.

--interpreter =[python|busybox]	Especifica el intérprete que se usará. El valor predeterminado es busybox.

%post (opcional)

Ejecuta el script especificado después de que finaliza la instalación del paquete. Si se especifican varias secciones `%post`, se ejecutan en el orden en que aparecen en el script de instalación.

--interpreter	Especifica el intérprete que se usará. El valor predeterminado es busybox.

`=[python|busybox]`	
`--timeout=secs`	Especifica el límite de tiempo de espera para la ejecución del script. Si el script no ha finalizado cuando se agota el tiempo de espera, se interrumpe de manera forzosa.
`--ignorefailure =[true|false]`	Si se configura como true, la instalación se considera correcta aunque el script `%post` haya terminado con un error.

%firstboot

Crea un script `init` que se ejecuta solamente durante el primer arranque. El script no afecta los arranques posteriores. Si se especifican varias secciones `%firstboot`, se ejecutan en el orden en que aparecen en el archivo de inicio.

Nota No es posible comprobar la semántica de los scripts `%firstboot` hasta el primer arranque del sistema. Un script `%firstboot` puede contener errores potencialmente catastróficos que no se detectan sino hasta después de la finalización de la instalación.

Importante El script `%firstboot` no se ejecuta si el arranque seguro está habilitado en el host ESXi.

`--interpreter =[python|busybox]`	Especifica el intérprete que se usará. El valor predeterminado es busybox.

Nota No es posible comprobar la semántica del script `%firstboot` hasta el primer arranque del sistema. Si el script contiene errores, no se detectan sino hasta después de la finalización de la instalación.

Nombre de los dispositivos de disco

Para los comandos del script de instalación `install`, `upgrade` e `installorupgrade`, es necesario usar los nombres de dispositivos de disco.

Tabla 2-13. Nombre de los dispositivos de disco

Formato	Ejemplo	Descripción
VML	vml.00025261	El nombre del dispositivo que indica el VMkernel
MPX	mpx.vmhba0:C0:T0:L0	El nombre del dispositivo

Acerca del archivo boot.cfg

El archivo de configuración del cargador de arranque `boot.cfg` especifica el kernel, las opciones del kernel y los módulos de arranque que utiliza el cargador de arranque `mboot.c32` o `mboot.efi` en una instalación de ESXi.

El archivo `boot.cfg` se incluye en el instalador de ESXi. Puede modificar la línea `kernelopt` del archivo `boot.cfg` para especificar la ubicación de un script de instalación o para pasar otras opciones de arranque.

El archivo `boot.cfg` tiene la siguiente sintaxis:

```
# boot.cfg -- mboot configuration file
#
# Any line preceded with '#' is a comment.

title=STRING
prefix=DIRPATH
kernel=FILEPATH
kernelopt=STRING
modules=FILEPATH1 --- FILEPATH2... --- FILEPATHn

# Any other line must remain unchanged.
```

Los comandos de `boot.cfg` configuran el cargador de arranque.

Tabla 2-14. Comandos de `boot.cfg`.

Comando	Descripción
`title=`*`STRING`*	Establece el título del cargador de arranque como *`STRING`*.
`prefix=`*`STRING`*	(Opcional) Agrega*`DIRPATH/`* frente a cada *`FILEPATH`* en los comandos `kernel=` y `modules=` que no empiezan con / o con `http://`.
`kernel=`*`FILEPATH`*	Establece la ruta de acceso del kernel como *`FILEPATH`*.
`kernelopt=`*`STRING`*	Anexa *`STRING`* a las opciones de arranque del kernel.
`modules=`*`FILEPATH1`* `---` *`FILEPATH2...`* `---` *`FILEPATHn`*	Enumera los módulos que se van a cargar, separados por tres guiones (`---`).

Consulte Crear una imagen ISO de instalador con un script de instalación o actualización personalizado y Arranque PXE del instalador de ESXi.

Instalar o actualizar ESXi desde un CD o DVD con un script

Puede instalar o actualizar ESXi desde una unidad de CD-ROM o DVD-ROM utilizando un script que especifique las opciones de instalación o actualización.

Puede iniciar el script de instalación o actualización introduciendo una opción de arranque cuando inicie el host. También puede crear una imagen ISO de instalador que incluya el script de instalación. Puede utilizar una imagen ISO de instalador para realizar una instalación generada por script y desatendida cuando arranque con la imagen ISO de instalador resultante. Consulte Crear una imagen ISO de instalador con un script de instalación o actualización personalizado.

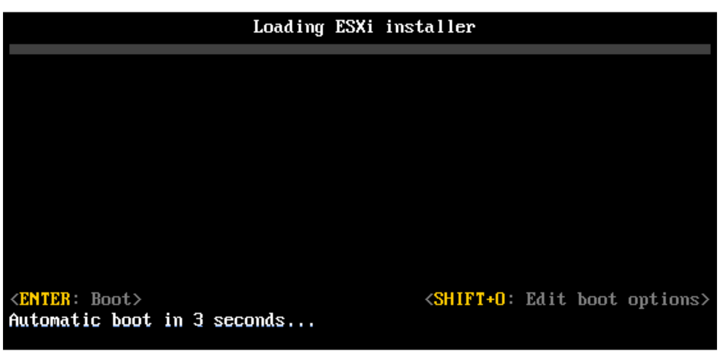
Requisitos previos

Antes de ejecutar la instalación o la actualización generadas por script, asegúrese de que se cumplen los siguientes requisitos previos:

- El sistema en el que va a realizar la instalación o actualización cumple con los requisitos de hardware. Consulte Requisitos de hardware de ESXi.
- Tiene el ISO con el instalador de ESXi en un CD o DVD de instalación. Consulte Descargar y grabar un CD or DVD de la imagen ISO del instalador de ESXi.
- El sistema puede acceder al script de instalación o actualización predeterminado (`ks.cfg`) o a un script de instalación o actualización personalizado. Consulte Acerca de los scripts de instalación y actualización.
- Ha seleccionado un comando de arranque para ejecutar la instalación o actualización generada por script. Consulte Introducir las opciones de arranque para iniciar un script de instalación o actualización. Para obtener una lista completa de los comandos de arranque, consulte Opciones de arranque .

Procedimiento

1. Arranque el instalador de ESXi desde la unidad de CD-ROM o DVD-ROM local.
2. Cuando aparezca la ventana del instalador de ESXi, presione las teclas Mayús + O para editar las opciones de arranque.



3. Introduzca una opción de arranque que invoque al archivo de script de instalación o actualización predeterminado o uno que haya creado.

   La opción de arranque tiene el formato `ks=`.
4. Presione Intro.

Resultados

Se ejecuta la operación de instalación, actualización o migración, utilizando las opciones que especificó.

Instalar o actualizar ESXi desde una unidad flash USB mediante un script

Puede instalar o actualizar ESXi desde una unidad flash USB utilizando un script que especifique las opciones de instalación o actualización.

Las opciones de arranque compatibles se detallan en Opciones de arranque .

Requisitos previos

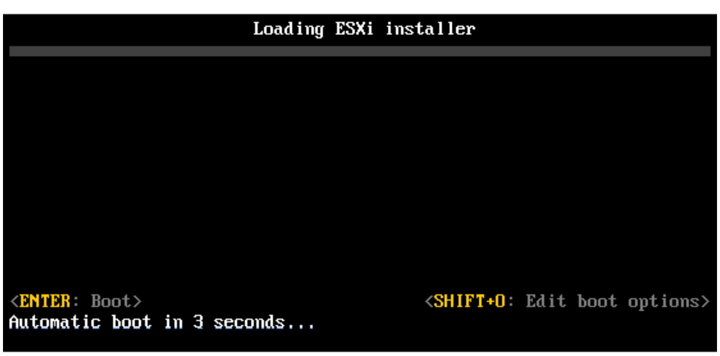
Antes de ejecutar la instalación o la actualización generadas por script, asegúrese de que se cumplen los siguientes requisitos previos:

- El sistema en el que va a realizar la instalación o la actualización a ESXi cumple con los requisitos de hardware para la instalación o la actualización. Consulte Requisitos de hardware de ESXi.
- Tiene el ISO con el instalador de ESXi en una unidad USB flash de arranque. Consulte Formatear una unidad flash USB para arrancar la instalación o la actualización de ESXi.
- El sistema puede acceder al script de instalación o actualización predeterminado (`ks.cfg`) o a un script de instalación o actualización personalizado. Consulte Acerca de los scripts de instalación y actualización.
- Ha seleccionado una opción de arranque para ejecutar la instalación, la actualización o la migración generadas por script. Consulte Introducir las opciones de arranque para iniciar un script de instalación o actualización.

Procedimiento

1 Arranque el instalador de ESXi desde la unidad flash USB.

2 Cuando aparezca la ventana del instalador de ESXi, presione las teclas Mayús + O para editar las opciones de arranque.



3 Introduzca una opción de arranque que invoque al archivo de script de instalación o actualización predeterminado o uno que haya creado.

La opción de arranque tiene el formato `ks=`.

4 Presione Intro.

Resultados

Se ejecuta la operación de instalación, actualización o migración, utilizando las opciones que especificó.

Realizar una instalación o actualización generada por script de ESXi a través de PXE para arrancar el instalador

ESXi 6.5 ofrece varias opciones para utilizar PXE para arrancar el instalador y utilizar un script de instalación o actualización.

- Para obtener información sobre la configuración de una infraestructura PXE, consulte Arranque PXE del instalador de ESXi.
- Para obtener información sobre la creación y ubicación de un script de instalación, consulte Acerca de los scripts de instalación y actualización.
- Para procedimientos específicos para utilizar PXE para arrancar el instalador de ESXi y utilizar un script de instalación, consulte uno de los siguientes temas:
  - Arranque PXE del instalador de ESXi mediante un servidor web
  - Arranque PXE del instalador de ESXi mediante TFTP
- Para obtener información sobre la utilización de vSphere Auto Deploy para realizar una instalación generada por script a través de PXE para arrancar, consulte Instalar ESXi con vSphere Auto Deploy .

Arranque PXE del instalador de ESXi

Es posible usar el entorno de ejecución previo al inicio (PXE) para arrancar un host. A partir de vSphere 6.0, es posible arrancar con PXE el instalador de ESXi desde una interfaz de red en los hosts con BIOS heredado o mediante UEFI.

ESXi se distribuye en un formato ISO que está diseñado para instalarse en la memoria flash o en un disco duro local. Puede extraer los archivos y arrancar con PXE.

PXE utiliza el protocolo de configuración dinámica de host (DHCP) y el protocolo trivial de transferencia de archivos (TFTP) para arrancar un sistema operativo a través de una red.

El arranque con PXE requiere determinada infraestructura de red y una máquina con un adaptador de red compatible con PXE. La mayoría de las máquinas que pueden ejecutar ESXi poseen adaptadores de red que pueden arrancar con PXE.

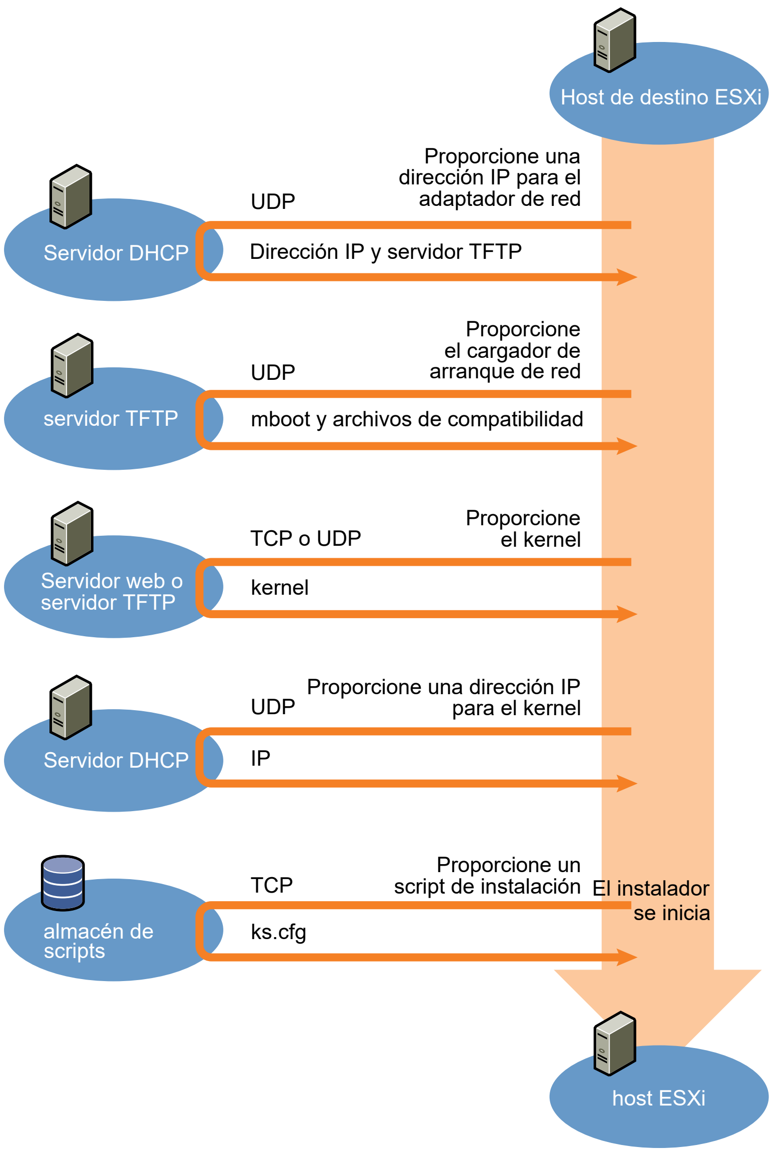
Nota El arranque PXE con firmware de BIOS heredado solo se puede realizar mediante IPv4. El arranque PXE con firmware UEFI se puede realizar mediante IPv4 o IPv6.

Descripción general de la instalación para el arranque PXE

Algunos de los detalles del proceso de arranque PXE varían si el host de destino utiliza firmware de UEFI o BIOS heredado y si el proceso de arranque utiliza solo TFTP o TFTP con HTTP.

Cuando se arranca el host de destino, este host interactúa con los diversos servidores en el entorno para obtener el adaptador de red, el cargador de arranque, el kernel, la dirección IP del kernel y el script de instalación. Una vez obtenidos todos los componentes, se inicia la instalación, como se muestra en la siguiente ilustración.

Figura 2-3. Descripción general de la instalación del arranque PXE



La interacción entre el host ESXi y los otros servidores continúa de la siguiente manera:

1 El usuario arranca el host ESXi de destino.

2 El host ESXi de destino realiza una solicitud DHCP.

3 El servidor DHCP responde con la información de IP y la ubicación del servidor TFTP.

4 El host ESXi se pone contacto con el servidor TFTP y solicita el archivo que especificó el servidor DHCP.

5 El servidor TFTP envía el cargador de arranque de red y el host ESXi lo ejecuta. Es posible que el cargador de arranque inicial cargue componentes de cargador de arranque adicionales del servidor TFTP.

6 El cargador de arranque busca un archivo de configuración en el servidor TFTP, descarga el kernel y otros componentes de ESXi del servidor HTTP o del servidor TFTP e inicia el kernel en el host ESXi.

7 El instalador se ejecuta de forma interactiva o mediante un script de inicio, según se especifique en el archivo de configuración.

Arranque PXE del instalador de ESXi mediante TFTP

Es posible utilizar un servidor TFTP para arrancar con PXE el instalador de ESXi. El proceso varía levemente si se utiliza UEFI o el arranque desde un BIOS heredado. Puesto que la mayoría de los entornos contienen tanto hosts ESXi compatibles con el arranque UEFI como hosts compatibles solo con el BIOS heredado, en este tema se analizan los requisitos previos y los pasos para ambos tipos de hosts.

- En los equipos con BIOS heredado, el procedimiento admite el arranque de varias versiones del instalador de ESXi con el mismo cargador de arranque inicial `pxelinux.0` o `gpxelinux.0` para todos los equipos de destino, pero con archivos de configuración PXELINUX potencialmente diferentes según la dirección MAC de los equipos de destino.
- En los equipos con UEFI, el procedimiento admite el arranque de varias versiones diferentes del instalador de ESXi con el mismo cargador de arranque inicial `mboot.efi` para todos los equipos de destino, pero con archivos `boot.cfg` potencialmente diferentes según la dirección MAC de los equipos de destino.

Requisitos previos

Compruebe que el entorno cumpla con los siguientes requisitos previos.

- Imagen ISO del instalador de ESXi descargada del sitio web de VMware.
- Host de destino con una configuración de hardware que sea compatible con la versión de ESXi. Consulte la *Guía de compatibilidad de VMware*.
- Un adaptador de red compatible con PXE en el host ESXi de destino.
- Un servidor DHCP configurado para el arranque PXE. Consulte Configuraciones de DHCP de muestra.
- Servidor TFTP.
- Directivas de seguridad de red para permitir el tráfico TFTP (Puerto UDP 69).
- Para BIOS heredado, solo se pueden usar redes IPv4. Para el arranque PXE con UEFI, se pueden usar redes IPv4 o IPv6.
- (Opcional) Un script de instalación (archivo de inicio).

- En la mayoría de los casos debe usar una VLAN nativa. Si desea especificar el identificador de la VLAN que se va a utilizar con el arranque PXE, compruebe que su NIC admita la especificación de identificador de la VLAN.

Para los sistemas BIOS heredados, obtenga la versión 3.86 del paquete SYSLINUX, disponible en https://www.kernel.org/pub/linux/utils/boot/syslinux/.

Procedimiento

1 Configure el servidor DHCP para el arranque TFTP.

2 (Solo BIOS heredado) Obtenga y configure PXELINUX:

   a Obtenga la versión 3.86 de SYSLINUX, descomprima el paquete y copie el archivo `pxelinux.0` en el directorio de nivel superior `/tftpboot` de su servidor TFTP.

   b Cree un archivo de configuración PXELINUX con el siguiente modelo de código.

   `ESXi-6.x.x-XXXXXX` es el nombre del subdirectorio TFTP donde se encuentran los archivos del instalador de ESXi.

```
DEFAULT install
NOHALT 1
LABEL install
  KERNEL ESXi-6.x.x-XXXXXX/mboot.c32
  APPEND -c ESXi-6.x.x-XXXXXX/boot.cfg
  IPAPPEND 2
```

   c Guarde el archivo PXELINUX en el directorio `/tftpboot/pxelinux.cfg` de su servidor TFTP con un nombre de archivo que determine si todos los hosts arrancarán este instalador de forma predeterminada:

Opción	Descripción
Mismo instalador	Use el nombre `default` para el archivo si desea que todos los hosts arranquen este instalador de ESXi de forma predeterminada.
Diferentes instaladores	Use la dirección MAC del equipo host de destino (01-*mac_address_of_target_ESXi_host*) como nombre para el archivo si desea que solo un host específico arranque con este archivo (por ejemplo, `01-23-45-67-89-0a-bc`).

3 (Solo UEFI) Copie el archivo `efi/boot/bootx64.efi` de la imagen ISO del instalador de ESXi en `/tftpboot/mboot.efi` en el servidor TFTP.

Nota Generalmente, las versiones más recientes de `mboot.efi` pueden arrancar versiones anteriores de ESXi, pero es posible que las versiones anteriores de `mboot.efi` no puedan arrancar versiones más recientes de ESXi. Si desea configurar diversos hosts de manera que arranquen diferentes versiones del instalador de ESXi, utilice el archivo `mboot.efi` de la versión más reciente.

4 Cree un subdirectorio en el directorio de nivel superior del servidor TFTP `/tftpboot` con el nombre de la versión de ESXi que almacenará, por ejemplo, `/tftpboot/ESXi-6.x.x-xxxxx`.

5 Copie el contenido de la imagen del instalador de ESXi en el directorio que acaba de crear.

6 Modifique el archivo `boot.cfg`.

   a Agregue la siguiente línea siguiente:

   ```
   prefix=ESXi-6.x.x-xxxxxx
   ```

   Aquí, `ESXi-6.x.x-xxxxxx` es el nombre de la ruta de acceso de los archivos del instalador en el directorio raíz del servidor TFTP.

   b Si los nombres de archivo en las líneas `kernel=` y `modules=` comienzan con un carácter de barra diagonal (/), elimine ese carácter.

7 (opcional) En el caso de una instalación generada por script, en el archivo `boot.cfg`, agregue la opción `kernelopt` en la línea siguiente al comando del kernel, para especificar la ubicación del script de instalación.

   Utilice el siguiente código como modelo, donde `XXX.XXX.XXX.XXX` es la dirección IP del servidor en el que reside el script de instalación y `esxi_ksFiles` es el directorio que contiene el archivo `ks.cfg`.

   ```
   kernelopt=ks=http://XXX.XXX.XXX.XXX/esxi_ksFiles/ks.cfg
   ```

8 (Solo UEFI) Especifique si desea que todos los hosts UEFI arranquen el mismo instalador.

Opción	Descripción
Mismo instalador	Copie el archivo `boot.cfg` en `/tftpboot/boot.cfg` o vincúlelo a esta ruta.
Diferentes instaladores	a Cree un subdirectorio de `/tftpboot` con la dirección MAC del equipo host de destino (01-*mac_address_of_target_ESXi_host*) como nombre (por ejemplo, `01-23-45-67-89-0a-bc`). b Coloque una copia (o un vínculo) del archivo `boot.cfg` del host en ese directorio (por ejemplo, `/tftpboot/01-23-45-67-89-0a-bc/boot.cfg`).

Arranque PXE del instalador de ESXi mediante un servidor web

Es posible utilizar un servidor web para arrancar el instalador de ESXi con PXE. Puesto que la mayoría de los entornos contienen tanto hosts ESXi compatibles con el arranque UEFI como hosts compatibles solo con el BIOS heredado, en este tema se analizan los requisitos previos y los pasos para ambos tipos de hosts.

- En los equipos con BIOS heredado, el procedimiento admite el arranque de varias versiones del instalador de ESXi con el mismo cargador de arranque inicial `pxelinux.0` o `gpxelinux.0` para todos los equipos de destino, pero con archivos de configuración PXELINUX potencialmente diferentes según la dirección MAC de los equipos de destino.

- En los equipos con UEFI, el procedimiento admite el arranque de varias versiones diferentes del instalador de ESXi con el mismo cargador de arranque inicial `mboot.efi` para todos los equipos de destino, pero con archivos `boot.cfg` potencialmente diferentes según la dirección MAC de los equipos de destino.

Requisitos previos

Compruebe que el entorno tenga los siguientes componentes:

- Imagen ISO del instalador de ESXi descargada del sitio web de VMware.
- Host de destino con una configuración de hardware que sea compatible con la versión de ESXi. Consulte la *Guía de compatibilidad de VMware*.
- Un adaptador de red compatible con PXE en el host ESXi de destino.
- Un servidor DHCP configurado para el arranque PXE. Consulte Configuraciones de DHCP de muestra.
- Servidor TFTP.
- Directivas de seguridad de red para permitir el tráfico TFTP (Puerto UDP 69).
- Para BIOS heredado, solo se pueden usar redes IPv4. Para el arranque PXE con UEFI, se pueden usar redes IPv4 o IPv6.
- (Opcional) Un script de instalación (archivo de inicio).
- En la mayoría de los casos debe usar una VLAN nativa. Si desea especificar el identificador de la VLAN que se va a utilizar con el arranque PXE, compruebe que su NIC admita la especificación de identificador de la VLAN.

Asegúrese de que el entorno también cumpla con los siguientes requisitos previos para el arranque PXE mediante un servidor web:

- Compruebe que los hosts ESXi de destino puedan acceder al servidor web HTTP.
- (UEFI) Obtenga iPXE, disponible en http://ipxe.org.
- (BIOS heredado) Obtenga la versión 3.86 del paquete SYSLINUX, disponible en https://www.kernel.org/pub/linux/utils/boot/syslinux/.

Procedimiento

1. Configure el servidor DHCP para el arranque HTTP.
2. (Solo UEFI) Obtenga y configure iPXE:
   a. Obtenga el código fuente de iPXE, tal como se describe en http://ipxe.org/download.
   b. Siga las instrucciones de esa página, pero utilice el siguiente comando make:

      ```
      make bin-x86_64-efi/snponly.efi
      ```

   c. Copie el archivo resultante `snponly.efi` en el directorio `/tftpboot` del servidor TFTP.

3 (Solo UEFI) Copie el archivo `efi/boot/bootx64.efi` de la imagen ISO del instalador de ESXi en `/tftpboot/mboot.efi` en el servidor TFTP.

Nota Generalmente, las versiones más recientes de `mboot.efi` pueden arrancar versiones anteriores de ESXi, pero es posible que las versiones anteriores de `mboot.efi` no puedan arrancar versiones más recientes de ESXi. Si desea configurar diversos hosts de manera que arranquen diferentes versiones del instalador de ESXi, utilice el archivo `mboot.efi` de la versión más reciente.

4 (Solo BIOS heredado) Obtenga y configure PXELINUX:

a Obtenga la versión 3.86 de SYSLINUX, descomprima el paquete y copie el archivo `gpxelinux.0` en el directorio de nivel superior `/tftpboot` de su servidor TFTP.

b Cree un archivo de configuración PXELINUX con el siguiente modelo de código.

`ESXi-6.x.x-XXXXXX` es el nombre del subdirectorio TFTP donde se encuentran los archivos del instalador de ESXi.

```
DEFAULT install
NOHALT 1
LABEL install
  KERNEL ESXi-6.x.x-XXXXXX/mboot.c32
  APPEND -c ESXi-6.x.x-XXXXXX/boot.cfg
  IPAPPEND 2
```

c Guarde el archivo PXELINUX en el directorio `/tftpboot/pxelinux.cfg` de su servidor TFTP con un nombre de archivo que determine si todos los hosts arrancarán este instalador de forma predeterminada:

Opción	Descripción
Mismo instalador	Use el nombre `default` para el archivo si desea que todos los hosts arranquen este instalador de ESXi de forma predeterminada.
Diferentes instaladores	Use la dirección MAC del equipo host de destino (01-*mac_address_of_target_ESXi_host*) como nombre para el archivo si desea que solo un host específico arranque con este archivo (por ejemplo, `01-23-45-67-89-0a-bc`).

5 Cree un directorio en su servidor HTTP con el nombre de la versión de ESXi que almacenará (por ejemplo, `/var/www/html/ESXi-6.x.x-XXXXXX`).

6 Copie el contenido de la imagen del instalador de ESXi en el directorio que acaba de crear.

7 Modifique el archivo `boot.cfg`.

   a Agregue la siguiente línea:

   ```
   prefix=http://XXX.XXX.XXX.XXX/ESXi-6.x.x-XXXXXX
   ```

   En la línea superior, `http://XXX.XXX.XXX.XXX/ESXi-6.x.x-XXXXXX` es la ubicación de los archivos del instalador en el servidor HTTP.

   b Si los nombres de archivo en las líneas `kernel=` y `modules=` comienzan con un carácter de barra diagonal (/), elimine ese carácter.

8 (opcional) En el caso de una instalación generada por script, en el archivo `boot.cfg`, agregue la opción `kernelopt` en la línea siguiente al comando del kernel, para especificar la ubicación del script de instalación.

   Utilice el siguiente código como modelo, donde `XXX.XXX.XXX.XXX` es la dirección IP del servidor en el que reside el script de instalación y `esxi_ksFiles` es el directorio que contiene el archivo `ks.cfg`.

   ```
   kernelopt=ks=http://XXX.XXX.XXX.XXX/esxi_ksFiles/ks.cfg
   ```

9 (Solo UEFI) Especifique si desea que todos los hosts UEFI arranquen el mismo instalador.

Opción	Descripción
Mismo instalador	Copie el archivo `boot.cfg` en `/tftpboot/boot.cfg` o vincúlelo a esta ruta.
Diferentes instaladores	a Cree un subdirectorio de `/tftpboot` con la dirección MAC del equipo host de destino (01-*mac_address_of_target_ESXi_host*) como nombre (por ejemplo, `01-23-45-67-89-0a-bc`). b Coloque una copia (o un vínculo) del archivo `boot.cfg` del host en ese directorio (por ejemplo, `/tftpboot/01-23-45-67-89-0a-bc/boot.cfg`).

Instalar ESXi con vSphere Auto Deploy

vSphere Auto Deploy permite aprovisionar cientos de hosts físicos con el software ESXi.

Mediante el uso de Auto Deploy, los administradores de sistemas experimentados pueden administrar de forma eficiente implementaciones grandes. Los hosts se arrancan mediante la red desde un servidor Auto Deploy central. De forma opcional, se configuran los hosts con un perfil de host de un host de referencia. El perfil de host se puede configurar para que le solicite al usuario información. Después que concluya el arranque y la configuración, los hosts los administra vCenter Server al igual que otros hosts ESXi.

Auto Deploy también se puede utilizar para almacenamientos en caché sin estado o instalaciones con estado.

Importante Auto Deploy requiere una separación segura entre la red de producción y las redes de administración o implementación, según se describe en Consideraciones de seguridad de vSphere Auto Deploy. No es seguro utilizar Auto Deploy sin esta separación.

Almacenamiento en caché sin estado

De manera predeterminada, Auto Deploy no almacena la configuración o estado de ESXi en el disco host. En su lugar, un perfil de imagen define la imagen con la que se aprovisiona el host. Los otros atributos de host se administran mediante perfiles de host. El host que utiliza Auto Deploy para el almacenamiento en caché sin estado debe conectarse al servidor Auto Deploy y a vCenter Server.

Instalaciones con estado

Puede aprovisionar un host con Auto Deploy y configurar el host para que almacene la imagen en el disco. En los arranques posteriores, el host lo hará desde el disco.

Información sobre vSphere Auto Deploy

vSphere Auto Deploy puede aprovisionar cientos de hosts físicos con el software ESXi. Se puede especificar la imagen que se implementará y los hosts que se aprovisionarán con esa imagen. Opcionalmente, puede especificar perfiles para aplicar a los hosts, una ubicación de vCenter Server (centro de datos, carpeta o clúster) y asignar un paquete de scripts para cada host.

Introduction to vSphere Auto Deploy

When you start a physical host that is set up for vSphere Auto Deploy, vSphere Auto Deploy uses PXE boot infrastructure in conjunction with vSphere host profiles to provision and customize that host. No state is stored on the host itself. Instead, the vSphere Auto Deploy server manages state information for each host.

State Information for ESXi Hosts

vSphere Auto Deploy stores the information for the ESXi hosts to be provisioned in different locations. Information about the location of image profiles and host profiles is initially specified in the rules that map machines to image profiles and host profiles.

Tabla 2-15. vSphere Auto Deploy Stores Information for Deployment

Information Type	Description	Source of Information
Image state	The executable software to run on an ESXi host.	Image profile, created with vSphere ESXi Image Builder.
Configuration state	The configurable settings that determine how the host is configured, for example, virtual switches and their settings, driver settings, boot parameters, and so on.	Host profile, created by using the host profile UI. Often comes from a template host.

Tabla 2-15. vSphere Auto Deploy Stores Information for Deployment (continuación)

Information Type	Description	Source of Information
Dynamic state	The runtime state that is generated by the running software, for example, generated private keys or runtime databases.	Host memory, lost during reboot.
Virtual machine state	The virtual machines stored on a host and virtual machine autostart information (subsequent boots only).	Virtual machine information sent by vCenter Server to vSphere Auto Deploy must be available to supply virtual machine information to vSphere Auto Deploy.
User input	State that is based on user input, for example, an IP address that the user provides when the system starts up, cannot automatically be included in the host profile.	Host customization information, stored by vCenter Server during first boot. You can create a host profile that requires user input for certain values. When vSphere Auto Deploy applies a host profile that requires user provided information, the host is placed in maintenance mode. Use the host profile UI to check the host profile compliance, and respond to the prompt to customize the host.

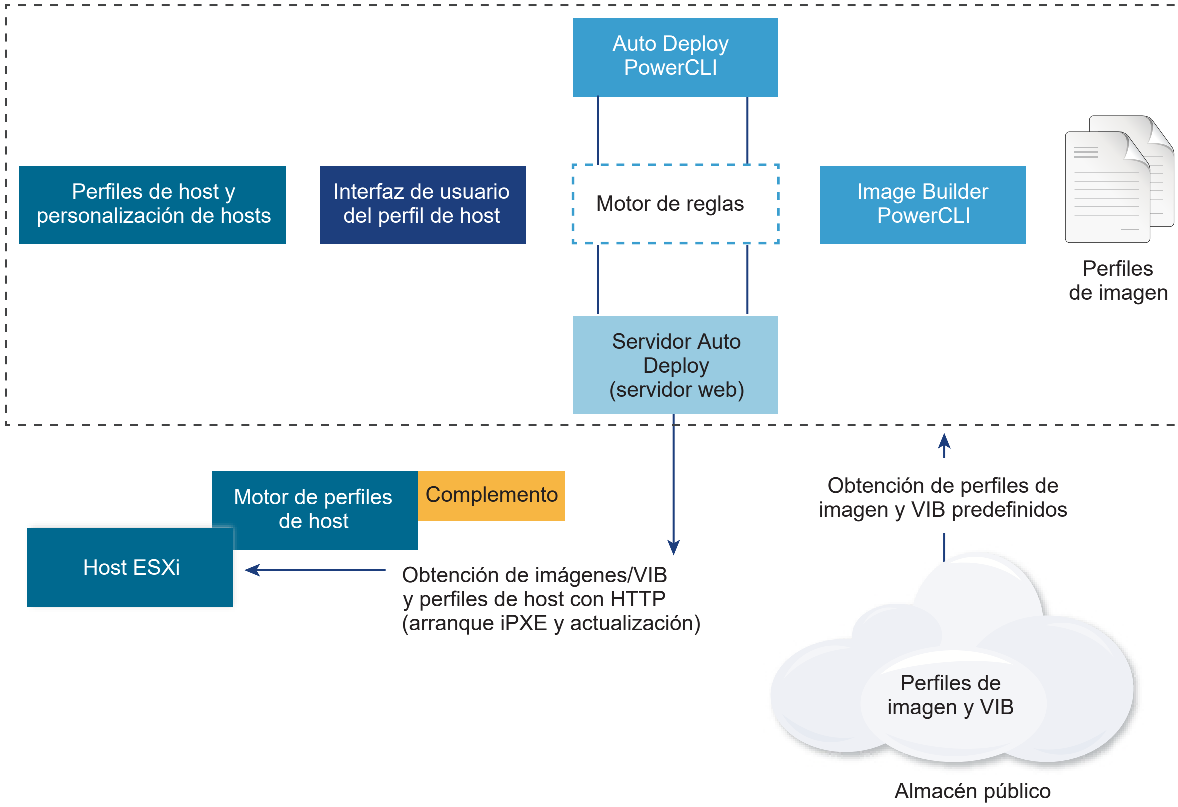
vSphere Auto Deploy Architecture

The vSphere Auto Deploy infrastructure consists of several components.

For more information, watch the video "Auto Deploy Architecture":

Auto Deploy Architecture
(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_i4ajkcm2/uiConfId/49694343/)

Figura 2-4. vSphere Auto Deploy Architecture



vSphere Auto Deploy server

Serves images and host profiles to ESXi hosts.

vSphere Auto Deploy rules engine

Sends information to the vSphere Auto Deploy server which image profile and which host profile to serve to which host. Administrators use vSphere Auto Deploy to define the rules that assign image profiles and host profiles to hosts. For more information on vSphere Auto Deploy rules and rule sets, see Reglas y conjuntos de reglas.

Image profiles

Define the set of VIBs to boot ESXi hosts with.

- VMware and VMware partners make image profiles and VIBs available in public depots. Use vSphere ESXi Image Builder to examine the depot and use the vSphere Auto Deploy rules engine to specify which image profile to assign to which host.
- VMware customers can create a custom image profile based on the public image profiles and VIBs in the depot and apply that image profile to the host. See Personalizar instalaciones con vSphere ESXi Image Builder.

Host profiles

Define machine-specific configuration such as networking or storage setup. Use the host profile UI to create host profiles. You can create a host profile for a reference host and apply that host profile to other hosts in your environment for a consistent configuration. For more information, see the *Perfiles de host de vSphere* documentation or the Configurar un host de referencia de vSphere Auto Deploy section.

Host customization

Stores information that the user provides when host profiles are applied to the host. Host customization might contain an IP address or other information that the user supplied for that host. For more information about host customizations, see the *Perfiles de host de vSphere* documentation.

Host customization was called answer file in earlier releases of vSphere Auto Deploy.

Reglas y conjuntos de reglas

El comportamiento del servidor vSphere Auto Deploy se especifica con un conjunto de reglas. El motor de reglas de vSphere Auto Deploy comprueba el conjunto de reglas para patrones de host coincidentes a fin de decidir con qué elementos (perfil de imagen, perfil de host, ubicación de vCenter Server u objeto de script) se debe aprovisionar cada host.

El motor de reglas asigna parámetros de software y configuración a los hosts según los atributos del host. Por ejemplo, puede implementar perfiles de imagen o perfiles de host a dos clústeres de hosts escribiendo dos reglas, cada una de las cuales debe coincidir con la dirección de red de un clúster.

Para hosts que aún no se han agregado a un sistema vCenter Server, el servidor vSphere Auto Deploy comprueba con el motor de reglas antes de entregar información de perfiles de imagen, perfiles de host y ubicación de inventario a los hosts. Para hosts administrados por un sistema vCenter Server, se usa el perfil de imagen, perfil de host y ubicación de inventario que vCenter Server tiene almacenados en el objeto de host. Si modifica las reglas, puede usar los cmdlets de vSphere Web Client o vSphere Auto Deploy en una sesión de PowerCLI para probar y reparar el cumplimiento de reglas. Cuando se repara el cumplimiento de reglas para un host, se actualizan las asignaciones de perfil de imagen y perfil de host de ese host.

El motor de reglas incluye reglas y conjuntos de reglas.

Reglas

Las reglas pueden asignar perfiles de imagen y de host a un conjunto de hosts, o bien especificar la ubicación (carpeta o clúster) de un host en el sistema vCenter Server de destino. Una regla puede identificar hosts de destino mediante la dirección MAC de arranque, la información del SMBIOS, la UUID del BIOS, el proveedor, el modelo o la dirección IP de DHCP fija. En la mayoría de los casos, se aplican reglas a varios hosts. Las reglas se crean mediante los cmdlets de vSphere Web Client o vSphere Auto Deploy en una sesión de PowerCLI. Después de crear una regla, se la debe agregar a un conjunto de reglas. Solo se admiten dos conjuntos de reglas: el conjunto de reglas activas y el conjunto de reglas de trabajo. Una regla puede pertenecer a ambos conjuntos, al predeterminado o solo al conjunto de reglas de

trabajo. Una vez que la regla se agrega a un conjunto de reglas, ya no se puede cambiar. En su lugar, copie la regla y reemplace los elementos o los patrones en la copia. Si administra vSphere Auto Deploy con vSphere Web Client, puede editar una regla si se encuentra en estado inactivo.

Puede especificar los siguientes parámetros en una regla.

Parámetro	Descripción
Nombre	Nombre de la regla, especificado mediante el parámetro `–Name`.
Elemento	Un elemento o más, especificados mediante el parámetro `–Item`. Un elemento puede ser un perfil de imagen, un perfil de host, una ubicación en el inventario de vCenter Server (centro de datos, carpeta o clúster) para el host de destino o un script personalizado. Puede especificar varios elementos, separados por comas.
Patrón	El patrón especifica el host o el grupo de hosts a los que se aplica la regla. **vendor** Nombre del proveedor de la máquina. **model** Nombre del modelo de la máquina. **serie** Número de serie de la máquina. **hostname** Nombre de host de la máquina. **domain** Nombre del dominio. **ipv4** Dirección IPv4 de la máquina. **ipv6** Dirección IPv6 de la máquina. El arranque PXE con firmware de BIOS solo se puede realizar mediante IPv4; el arranque PXE con firmware de UEFI se puede realizar mediante IPv4 o IPv6. **mac** Dirección MAC de NIC de arranque. **asset** Etiqueta de recurso de la máquina. **oemstring** Cadenas específicas del fabricante del equipo original (OEM) en el SMBIOS. Puede especificar el parámetro `–AllHosts` para aplicar el elemento o los elementos a todos los hosts.

Conjunto de reglas activas

Cuando un host iniciado recientemente contacta al servidor vSphere Auto Deploy con una solicitud de perfil de imagen, el servidor vSphere Auto Deploy si hay reglas coincidentes en el conjunto de reglas activas. El perfil de imagen, el perfil de host, la ubicación de inventario de vCenter Server y el objeto de script que se asignan mediante reglas coincidentes se utilizan posteriormente para arrancar el host. Si las reglas asignan más de un elemento del mismo tipo, el servidor vSphere Auto Deploy utilizará el elemento que aparezca primero en el conjunto de reglas.

Conjunto de reglas de trabajo

El conjunto de reglas de trabajo permite probar cambios en las reglas antes de que se activen dichos cambios. Por ejemplo, puede usar cmdlets de vSphere Auto Deploy para probar el cumplimiento del conjunto de reglas de trabajo. La prueba verifica que los hosts administrados por un sistema vCenter Server sigan las reglas en el conjunto de reglas de trabajo. De manera predeterminada, los cmdlets agregan la regla al conjunto de reglas de trabajo y activan las reglas. Utilice el parámetro `NoActivate` para agregar una regla solamente al conjunto de reglas de trabajo.

Con las reglas y los conjuntos de reglas se usa el siguiente flujo de trabajo.

1 Haga cambios en el conjunto de reglas de trabajo.
2 Pruebe las reglas del conjunto de reglas de trabajo para un host a fin de garantizar que todo funcione correctamente.
3 Refine y vuelva a probar las reglas en el conjunto de reglas de trabajo.
4 Active las reglas en el conjunto de reglas de trabajo.

   Si agrega una regla en una sesión de PowerCLI y no especifica el parámetro `NoActivate`, se activan todas las reglas que se encuentran actualmente en el conjunto de reglas de trabajo. No puede activar reglas individuales.

Consulte la ayuda de la línea de comandos PowerCLI y Administrar vSphere Auto Deploy con cmdlets de PowerCLI para obtener más información sobre el uso de vSphere Auto Deploy con cmdlets de PowerCLI. Consulte Administrar vSphere Auto Deploy con vSphere Web Client para obtener más información sobre el uso de vSphere Auto Deploy con vSphere Web Client.

Proceso de arranque de vSphere Auto Deploy

Al arrancar un host que desea aprovisionar o reaprovisionar con vSphere Auto Deploy, la infraestructura de vSphere Auto Deploy suministra el perfil de imagen y, opcionalmente, un perfil de host, una ubicación de vCenter Server y un paquete de scripts para ese host.

El proceso de arranque para los hosts que aún no se han aprovisionado con vSphere Auto Deploy (primer arranque) es distinto al de los hosts que sí se aprovisionaron con vSphere Auto Deploy y se agregaron a un sistema vCenter Server (arranque posterior).

Requisitos previos para primer arranque

Antes de un proceso de primer arranque, debe configurar el sistema. La configuración incluye las siguientes tareas, que se tratan más detalladamente en Prepararse para vSphere Auto Deploy.

- Configure un servidor DHCP que asigne una dirección IP a cada host durante el inicio y que apunte el host al servidor TFTP desde el que se va a descargar el cargador de arranque iPXE.
- Si los hosts que planea aprovisionar con vSphere Auto Deploy presentan un BIOS heredado, compruebe que el servidor vSphere Auto Deploy tenga una dirección IPv4. El arranque PXE con firmware de BIOS heredado solo se puede realizar mediante IPv4. El arranque PXE con firmware UEFI se puede realizar mediante IPv4 o IPv6.
- Identifique el perfil de imagen que se va a usar de una de las siguientes maneras.
  - Elija un perfil de imagen de ESXi de un almacén público.
  - (opcional) Cree un perfil de imagen personalizado mediante vSphere ESXi Image Builder y colóquelo en un almacén al que pueda acceder el servidor vSphere Auto Deploy. El perfil de imagen debe incluir un VIB de ESXi de base.
- (opcional) Si tiene un host de referencia en el entorno, exporte el perfil de host de este y defina una regla que aplique el perfil a uno o más hosts. Consulte Configurar un host de referencia de vSphere Auto Deploy.
- Especifique reglas para la implementación del host y agréguelas al conjunto de reglas activo.

Información general sobre el primer arranque

Cuando se arranca un host que aún no se ha aprovisionado con arranques de vSphere Auto Deploy (primer arranque), el host interactúa con varios componentes de vSphere Auto Deploy.

1 Cuando el administrador enciende un host, este inicia una secuencia de arranque PXE.

   El servidor DHCP asigna una dirección IP al host y le indica que debe ponerse en contacto con el servidor TFTP.

2 El host realiza esta acción y descarga el archivo iPXE (cargador de arranque ejecutable) y un archivo de configuración iPXE.

3 iPXE comienza a ejecutarse.

   El archivo de configuración le indica al host que realice una solicitud de arranque HTTP al servidor vSphere Auto Deploy. La solicitud HTTP incluye información de hardware y de red.

4 En respuesta, el servidor vSphere Auto Deploy realiza estas tareas:

   a Consulta al motor de reglas la información sobre el host.

   b Transmite los componentes especificados en la información de perfil de imagen, perfil de host opcional y ubicación de vCenter Server opcional.

5 El host arranca mediante el perfil de imagen.

   Si el servidor vSphere Auto Deploy proporcionó un perfil de host, este se aplica al host.

6 vSphere Auto Deploy agrega el host al sistema vCenter Server en el que está registrado vSphere Auto Deploy.

   a Si una regla especifica una carpeta o un clúster de destino en el sistema vCenter Server, el host se coloca en esa carpeta o ese clúster. La carpeta de destino debe estar dentro de un centro de datos.

   b Si no existe una regla que especifique una ubicación de inventario de vCenter Server, vSphere Auto Deploy agrega el host al primer centro de datos que aparece en la interfaz de usuario de vSphere Web Client.

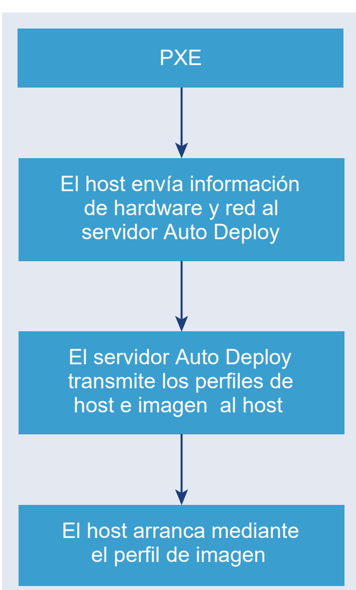
7 (opcional) Si el perfil de host requiere que el usuario especifique cierta información, como una dirección IP estática, el host se coloca en modo de mantenimiento cuando se agrega al sistema vCenter Server.

   Debe volver a aplicar el perfil de host y actualizar la personalización del host para que este salga del modo de mantenimiento. Al actualizar la personalización del host, debe responder las preguntas cuando se le pida.

8 Si el host forma parte de un clúster de DRS, las máquinas virtuales de otros hosts podrían migrarse al host después de que este se haya agregado correctamente al sistema vCenter Server.

Consulte Aprovisionar un host (primer arranque).

Figura 2-5. Instalación de vSphere Auto Deploy, primer arranque



Arranques posteriores sin actualizaciones

En el caso de los hosts aprovisionados con vSphere Auto Deploy y administrados por un sistema vCenter Server, los arranques posteriores pueden volverse completamente automáticos.

1 El administrador reinicia el host.

2 A medida que el host arranca, vSphere Auto Deploy lo aprovisiona con su perfil de imagen y su perfil de host.

3 Las máquinas virtuales se activan o se migran al host en base a la configuración del host.

- Host independiente. Las máquinas virtuales se encienden de acuerdo con las reglas de inicio automático definidas en el host.
- Host del clúster de DRS. Las máquinas virtuales que se migraron correctamente a otros hosts permanecen allí. Las máquinas virtuales para las que ningún host tenía recursos suficientes se registran en el host que se reinició.

Si el sistema vCenter Server no está disponible, el host se pone en contacto con el servidor vSphere Auto Deploy y se aprovisiona con un perfil de imagen. El host continúa poniéndose en contacto con el servidor vSphere Auto Deploy hasta que vSphere Auto Deploy vuelve a conectarse con el sistema vCenter Server.

vSphere Auto Deploy no puede configurar los conmutadores distribuidos de vSphere si vCenter Server no está disponible. Asimismo, las máquinas virtuales se asignan a hosts solo si forman parte de un clúster HA. Una vez que el host vuelva a conectarse a vCenter Server y se aplique el perfil de host, podrá crear el conmutador. Debido a que el host se encuentra en modo de mantenimiento, no es posible iniciar las máquinas virtuales. Consulte Reaprovisionar hosts con operaciones de reinicio simples.

Los hosts que están configurados para pedir intervención del usuario se colocan en modo de mantenimiento. Consulte Actualizar la personalización de hosts en vSphere Web Client.

Arranques posteriores con actualizaciones

Es posible cambiar el perfil de imagen, el perfil de host, la ubicación de vCenter Server o el paquete de scripts de los hosts. El proceso involucra cambiar reglas, así como probar y reparar el cumplimiento de reglas del host.

1 El administrador utiliza el cmdlet `Copy-DeployRule` de PowerCLI para copiar y editar una o más reglas. A continuación, actualiza el conjunto de reglas. Consulte Introducción al proceso de vSphere Auto Deploy con PowerCLI para ver un ejemplo.

2 El administrador ejecuta el cmdlet `Test-DeployRulesetCompliance` para comprobar si cada host utiliza la información que especifica el conjunto de reglas actual.

3 El host devuelve un objeto de PowerCLI que encapsula la información de cumplimiento.

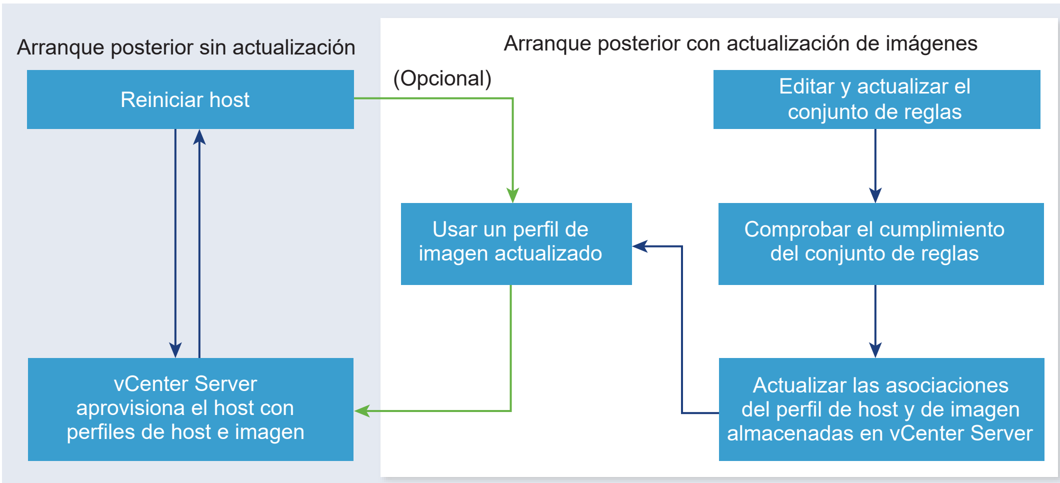
4 El administrador ejecuta el cmdlet `Repair-DeployRulesetCompliance` para actualizar el perfil de imagen, el perfil de host o la ubicación de vCenter Server que almacena el sistema vCenter Server para cada host.

5 Cuando el host se reinicia, utiliza el perfil de imagen, el perfil de host, la ubicación de vCenter Server o el paquete de scripts actualizados del host.

  Si el perfil de host está configurado para solicitar la intervención del usuario, el host se coloca en modo de mantenimiento. Siga los pasos descritos en Actualizar la personalización de hosts en vSphere Web Client.

Consulte Probar y reparar cumplimiento de reglas .

Figura 2-6. Instalación de vSphere Auto Deploy, arranques posteriores



Aprovisionar sistemas que tienen conmutadores distribuidos

Puede configurar el perfil de host de un host de referencia de vSphere Auto Deploy con un conmutador distribuido.

Cuando configura el conmutador distribuido, la directiva de parámetros de configuración de arranque se establece automáticamente para que coincida con los parámetros de red necesarios para la conectividad del host después de un reinicio.

Cuando vSphere Auto Deploy aprovisiona el host ESXi con el perfil de host, el host pasa por un proceso de dos pasos.

1 Crea un conmutador estándar virtual con las propiedades especificadas en el campo de parámetros de configuración de arranque.

2 Crea las NIC de VMkernel. Las NIC de VMkernel permiten que el host se conecte con vSphere Auto Deploy y el sistema vCenter Server.

Cuando el host se agrega a vCenter Server, vCenter Server elimina el conmutador estándar y vuelve a aplicar el conmutador distribuido al host.

Nota No modifique los parámetros de configuración de arranque del host para evitar problemas con el conmutador distribuido.

Introducción al proceso de vSphere Auto Deploy con vSphere Web Client

Para comenzar a usar vSphere Auto Deploy, debe aprender cómo funciona vSphere Auto Deploy, iniciar los servicios de vCenter Server vSphere ESXi Image Builder y vSphere Auto Deploy, escribir reglas de implementación que aprovisionen hosts y encender los hosts que deben arrancarse con el perfil de imagen especificado.

El flujo de trabajo para aprovisionar los hosts en su entorno con vSphere Auto Deploy incluye las siguientes tareas:

1 Instale vCenter Server y los componentes de vCenter Server, o implemente vCenter Server Appliance.

   El servidor vSphere Auto Deploy se incluye junto con el nodo de administración.

2 Configure los tipos de inicio de los servicios vSphere Auto Deploy y vSphere ESXi Image Builder.

   Consulte Preparar el sistema para vSphere Auto Deploy.

3 Agregue o importe un almacén de software al inventario de vSphere Auto Deploy.

   Consulte Agregar un almacén de software o Importar un almacén de software.

4 (Opcional) Si quiere crear un perfil de imagen personalizado, clone o cree un perfil de imagen con vSphere Web Client.

   Consulte Clonar un perfil de imagen o Crear un perfil de imagen.

5 Cree una regla de implementación que asigne el perfil de imagen a un host, a varios hosts especificados mediante un patrón o a todos los hosts.

   Consulte Crear una regla de implementación.

   Nota vSphere Auto Deploy se optimizó para aprovisionar hosts que contienen una dirección MAC fija a una asignación de dirección IP en DHCP (a veces se denominan reservas de DHCP). Si desea utilizar direcciones IP estáticas, debe configurar el perfil de host para que solicite la personalización del host. Para obtener más información, consulte la documentación sobre *Perfiles de host de vSphere*.

6 Encienda los hosts que desea aprovisionar.

7 Configure el host aprovisionado como host de referencia para el perfil de host.

   Puede especificar la configuración de Syslog del host de referencia, la configuración del firewall, el almacenamiento, las redes, etc.

8 Extraiga un perfil de host del host de referencia.

   Consulte la documentación sobre *perfiles de host*.

9 Para aprovisionar varios hosts con el perfil de host, clone o edite la regla creada anteriormente con vSphere Web Client.

   Consulte Clonar una regla de implementación o Editar una regla de implementación.

10 Active la nueva regla y desactive la anterior.

   Consulte Activar, desactivar y reordenar las reglas de implementación.

11 Corrija las asociaciones de host para aplicar la nueva regla al host.

   Consulte Corregir un host no compatible.

12 Compruebe que los hosts aprovisionados cumplan los siguientes requisitos:

- Cada host está conectado al sistema vCenter Server.
- Los hosts no están en modo de mantenimiento.
- Los hosts no presentan instancias de incumplimiento de normas.
- Cada host con un perfil de host que requiere entradas del usuario tiene información actualizada de personalización del host.

Corrija los problemas de cumplimiento y asociaciones de hosts, y reinicie los hosts hasta que todos los hosts cumplan con los requisitos.

Consulte para obtener una introducción al proceso de arranque, las diferencias entre el primer arranque y los arranques posteriores y una descripción general del uso de la personalización de hosts.

Introducción al proceso de vSphere Auto Deploy con PowerCLI

Para comenzar a usar vSphere Auto Deploy, debe aprender cómo funciona vSphere Auto Deploy, instalar el servidor vSphere Auto Deploy, instalar PowerCLI, escribir reglas de PowerCLI que aprovisionen hosts y encender los hosts que deben arrancarse con el perfil de imagen especificado. Puede personalizar el perfil de imagen, el perfil de host y la ubicación de vCenter Server.

Consulte Configurar vSphere Auto Deploy y aprovisionar hosts con vSphere PowerCLI para obtener un ejercicio paso a paso que le ayude a configurar su primer entorno de vSphere Auto Deploy en un sistema Windows Server 2008.

Para aprovisionar correctamente los hosts en su entorno con vSphere Auto Deploy, puede seguir estos pasos.

1 Instale vCenter Server y los componentes de vCenter Server, o implemente vCenter Server Appliance.

   El servidor vSphere Auto Deploy se incluye junto con el nodo de administración.

2 Configure el tipo de inicio para el servicio de vSphere Auto Deploy.

   Consulte Preparar el sistema para vSphere Auto Deploy.

3 Instale PowerCLI, que incluye cmdlets de vSphere Auto Deploy y vSphere ESXi Image Builder.

   Consulte Preparar el sistema para vSphere Auto Deploy y Usar los cmdlets de vSphere Auto Deploy.

4 Busque el perfil de imagen que incluye los VIB que desea implementar en los hosts.

   - En la mayoría de los casos, debe agregar los almacenes que contienen el software necesario a la sesión de PowerCLI y, a continuación, seleccionar un perfil de imagen desde uno de esos almacenes.

- Si desea crear un perfil de imagen personalizado, use los cmdlets de vSphere ESXi Image Builder para clonar un perfil de imagen existente y agregue los VIB personalizados al clon. Agregue el perfil de imagen personalizado a la sesión de PowerCLI.

Debe utilizar vSphere ESXi Image Builder para la personalización solamente si tiene que agregar o quitar VIB. En la mayoría de los casos, puede agregar el almacén en el que VMware aloja los perfiles de imagen a la sesión de PowerCLI como una URL.

5 Inicie una sesión de PowerCLI y conéctese con el sistema vCenter Server con el que vSphere Auto Deploy está registrado.

6 Use el cmdlet `New-DeployRule` de PowerCLI para escribir una regla que asigne el perfil de imagen a un host, a varios hosts especificados mediante un patrón o a todos los hosts.

```
New-DeployRule -Name "testrule" -Item image-profile -AllHosts
```

Consulte Asignar un perfil de imagen a hosts.

Nota vSphere Auto Deploy se optimizó para aprovisionar hosts que contienen una dirección MAC fija a una asignación de dirección IP en DHCP (a veces se denominan reservas de DHCP). Si desea utilizar direcciones IP estáticas, debe configurar el perfil de host para que solicite la personalización del host. Para obtener más información, consulte la documentación sobre *Perfiles de host de vSphere*.

7 Encienda los hosts que desea aprovisionar.

8 Configure el host aprovisionado como host de referencia para el perfil de host.

Puede especificar la configuración de Syslog del host de referencia, la configuración del firewall, el almacenamiento, las redes, etc.

9 Configure el host aprovisionado como host de referencia para el perfil de host.

Puede especificar la configuración de Syslog del host de referencia, la configuración del firewall, el almacenamiento, las redes, etc. Consulte Configurar un host de referencia de vSphere Auto Deploy.

10 Cree y exporte un perfil de host para el host de referencia.

Consulte la documentación sobre *perfiles de host*.

11 Para aprovisionar varios hosts con el perfil de host, use el cmdlet `Copy-DeployRule` para editar la regla creada anteriormente.

Puede revisar la regla para asignar no solo un perfil de imagen, sino también un perfil de host, una ubicación de vCenter Server y un paquete de scripts personalizado.

```
Copy-DeployRule -DeployRule "testrule" -ReplaceItem
my_host_profile_from_reference_host,my_target_cluster
               -ReplacePattern  "ipv4=192.XXX.1.10-192.XXX.1.20"
```

Donde *my_host_profile_from_reference_host* es el nombre del perfil de host de referencia y *my_target_cluster* es el nombre del clúster de destino.

12 Realice las operaciones de cumplimiento de prueba y reparación para corregir los hosts.

Consulte Probar y reparar cumplimiento de reglas .

13 Compruebe que los hosts aprovisionados cumplan los siguientes requisitos:

- Cada host está conectado al sistema vCenter Server.
- Los hosts no están en modo de mantenimiento.
- Los hosts no presentan instancias de incumplimiento de normas.
- Cada host con un perfil de host que requiere entradas del usuario tiene información actualizada de personalización del host.

Corrija los problemas de cumplimiento y asociaciones de hosts, y reinicie los hosts hasta que todos los hosts cumplan con los requisitos.

Consulte para obtener una introducción al proceso de arranque, las diferencias entre el primer arranque y los arranques posteriores y una descripción general del uso de la personalización de hosts.

Prepararse para vSphere Auto Deploy

Antes de comenzar a usar vSphere Auto Deploy, debe preparar el entorno. Comience con la configuración de los servidores y la preparación del hardware. Debe configurar el tipo de inicio para el servicio de vSphere Auto Deploy en el sistema vCenter Server que planea utilizar para administrar los hosts que aprovisione, y debe instalar PowerCLI.

- Preparar el sistema para vSphere Auto Deploy

  Para poder realizar un arranque PXE de un host ESXi con vSphere Auto Deploy, primero es necesario instalar el software de los requisitos previos y configurar los servidores DHCP y TFTP con los que deberá interactuar vSphere Auto Deploy.

- Usar los cmdlets de vSphere Auto Deploy

  Los cmdlets de vSphere Auto Deploy se implementan como cmdlets de Microsoft PowerShell y se incluyen en PowerCLI. Los usuarios de los cmdlets de vSphere Auto Deploy pueden aprovechar todas las funciones de PowerCLI.

- Configurar licencias masivas

  Puede utilizar vSphere Web Client o ESXi Shell para especificar claves de licencia individuales o configurar licencias masivas mediante los cmdlets de PowerCLI. Las licencias masivas funcionan para todos los hosts ESXi, pero son especialmente útiles para los hosts aprovisionados con vSphere Auto Deploy.

Preparar el sistema para vSphere Auto Deploy

Para poder realizar un arranque PXE de un host ESXi con vSphere Auto Deploy, primero es necesario instalar el software de los requisitos previos y configurar los servidores DHCP y TFTP con los que deberá interactuar vSphere Auto Deploy.

Requisitos previos

- Compruebe que los hosts que desea aprovisionar con vSphere Auto Deploy cumplan los requisitos de hardware para ESXi. Consulte Requisitos de hardware de ESXi.
- Compruebe que los hosts ESXi tengan conectividad de red con vCenter Server y que se cumplan todos los requisitos de puerto. Consulte Puertos necesarios para vCenter Server y Platform Services Controller.
- Si desea usar redes VLAN en el entorno de vSphere Auto Deploy, debe configurar las redes de extremo a extremo correctamente. Cuando el host realiza un arranque PXE, se debe configurar el controlador de firmware de manera que los marcos se etiqueten con los identificadores de VLAN apropiados. Debe realizar los cambios apropiados en la interfaz UEFI/BIOS de forma manual para establecer esta configuración. De forma similar, debe configurar los grupos de puertos de ESXi correctamente con los identificadores de VLAN adecuados. Póngase en contacto con su administrador de red para obtener más información sobre la manera en la que los identificadores de VLAN se utilizan en el entorno.
- Asegúrese de contar con suficiente espacio de almacenamiento para el repositorio de vSphere Auto Deploy. El servidor vSphere Auto Deploy utiliza el repositorio para almacenar los datos que necesita, incluidos las reglas y los conjuntos de reglas que usted crea, así como los VIB y los perfiles de imagen que se especifican en las reglas.

  Se recomienda asignar 2 GB para que haya suficiente espacio para almacenar cuatro perfiles de imagen y quede espacio adicional. Cada perfil de imagen requiere aproximadamente 350 MB. Determine la cantidad de perfiles de imagen que espera utilizar para definir la cantidad de espacio que debe reservar para el repositorio de vSphere Auto Deploy.
- Otorgue privilegios administrativos al servidor DHCP que administra el segmento de red desde el cual desea realizar el arranque. Puede utilizar un servidor DHCP que ya se encuentre en el entorno, o bien instalarlo. Para la instalación de vSphere Auto Deploy, reemplace el nombre de archivo `gpxelinux.0` por `snponly64.efi.vmw-hardwired` para UEFI o por `undionly.kpxe.vmw-hardwired` para BIOS. Para obtener más información sobre las configuraciones de DHCP, consulte Configuraciones de DHCP de muestra.
- Proteja la red de la misma manera que lo haría con cualquier otro método de implementación basado en PXE. vSphere Auto Deploy transfiere datos por SSL para evitar la interferencia y la intromisión casuales. No obstante, la autenticidad del cliente o del servidor vSphere Auto Deploy no se comprueba durante el arranque PXE.

- Si desea administrar vSphere Auto Deploy con cmdlets de PowerCLI, compruebe que Microsoft .NET Framework 4.5 o 4.5.x y Windows PowerShell 3.0 o 4.0 se encuentren instalados en un equipo Windows. Es posible instalar PowerCLI en el sistema Windows donde se encuentra instalado vCenter Server o en otro sistema Windows. Consulte *Guía del usuario de vSphere PowerCLI*.
- Configure un servidor remoto de Syslog. Consulte la documentación de *Administrar vCenter Server y hosts* para obtener información sobre la configuración del servidor de Syslog. Configure el primer host que arranque para que use el servidor remoto de Syslog y aplique el perfil de host de dicho host a todos los demás hosts de destino. También puede instalar y utilizar vSphere Syslog Collector, una herramienta de soporte de vCenter Server que proporciona una arquitectura unificada de registros del sistema y habilita el registro de red, así como la combinación de registros de varios hosts.
- Instale ESXi Dump Collector, configure el primer host de manera que todos los volcados de memoria del núcleo se direccionen a ESXi Dump Collector y aplique el perfil de host de ese host a todos los otros hosts. Consulte Configurar ESXi Dump Collector con ESXCLI .
- Si los hosts que planea aprovisionar con vSphere Auto Deploy presentan un BIOS heredado, compruebe que el servidor vSphere Auto Deploy tenga una dirección IPv4. El arranque PXE con firmware de BIOS heredado solo se puede realizar mediante IPv4. El arranque PXE con firmware UEFI se puede realizar mediante IPv4 o IPv6.

Procedimiento

1 Instale vCenter Server o implemente vCenter Server Appliance.

   El servidor vSphere Auto Deploy se incluye junto con el nodo de administración.

2 Configure el tipo de inicio para el servicio de vSphere Auto Deploy.

   a Inicie sesión en el sistema de vCenter Server mediante vSphere Web Client.

   b En la página de inicio de vSphere Web Client, haga clic en **Administración**.

   c En **Configuración del sistema**, haga clic en **Servicios**.

   d Seleccione **Auto Deploy**, haga clic en el menú **Acciones** y seleccione **Editar tipo de inicio**.

      - En Windows, el servicio de vSphere Auto Deploy se encuentra deshabilitado. En la ventana **Editar tipo de inicio**, seleccione **Manual** o **Automático** para habilitar vSphere Auto Deploy.
      - En vCenter Server Appliance, el servicio de vSphere Auto Deploy está establecido de forma predeterminada en **Manual**. Si desea que el servicio de vSphere Auto Deploy se inicie de manera automática al iniciar el sistema operativo, seleccione **Automático**.

3 (opcional) Si desea administrar vSphere Auto Deploy con vSphere Web Client, configure el tipo de inicio para el servicio de vSphere ESXi Image Builder.

   a Repita las operaciones del paso secundario 2a al paso secundario 2c.

   b Seleccione **Servicio de ImageBuilder**, haga clic en el menú **Acciones** y seleccione **Editar tipo de inicio**.

      - En Windows, el servicio de vSphere ESXi Image Builder se encuentra deshabilitado. En la ventana **Editar tipo de inicio**, seleccione **Manual** o **Automático** para habilitar el servicio.
      - En vCenter Server Appliance, el servicio de vSphere Auto Deploy está establecido de forma predeterminada en **Manual**. Si desea que el servicio de vSphere ESXi Image Builder se inicie de manera automática al iniciar el sistema operativo, seleccione **Automático**.

   c Cierre la sesión de vSphere Web Client y vuelva a iniciar sesión.

      El icono de **Auto Deploy** se mostrará en la página de inicio de vSphere Web Client.

4 (opcional) Si desea administrar vSphere Auto Deploy con cmdlets de PowerCLI, instale PowerCLI.

   a Descargue la versión más reciente de PowerCLI del sitio web de VMware.

   b Desplácese hasta la carpeta que contiene el archivo de PowerCLI que descargó y haga doble clic en el archivo ejecutable.

      Si el asistente de instalación detecta una versión anterior de PowerCLI en el sistema, el asistente intentará actualizar la instalación existente.

   c Siga las instrucciones del asistente para completar la instalación.

5 Configure el servidor TFTP.

   a En vSphere Web Client conectado al sistema de vCenter Server, seleccione el sistema de vCenter Server en la lista de inventario.

   b Haga clic en la pestaña **Administrar**, seleccione **Configuración** y haga clic en **Auto Deploy**.

   c Haga clic en **Descargar ZIP de arranque TFTP** para descargar el archivo de configuración de TFTP y, a continuación, descomprima el archivo en el directorio en el que el servidor TFTP almacena los archivos.

6 Configure el servidor DHCP de manera que apunte al servidor TFTP en el que se encuentra el archivo ZIP de TFTP.

   a Especifique la dirección IP del servidor TFTP en la opción 66 del DHCP, la cual se suele llamar next-server.

   b Especifique el nombre del archivo de arranque, que es `snponly64.efi.vmw-hardwired` para UEFI o `undionly.kpxe.vmw-hardwired` para BIOS en la opción 67 de DHCP, y se conoce comúnmente como `boot-filename`.

7 Configure todos los hosts que desea aprovisionar con vSphere Auto Deploy para realizar un arranque de red o un arranque PXE, según las instrucciones del fabricante.

8 (opcional) Si configura el entorno de manera que se utilice el modo de huellas digitales, puede reemplazar el certificado `rbd-ca.crt` de OpenSSL y la clave privada `rbd-ca.key` de OpenSSL por un certificado y una clave privada personales para utilizar su propia entidad de certificación (Certificate Authority, CA).

   - En Windows, los archivos se encuentran en la subcarpeta SSL del directorio de instalación de vSphere Auto Deploy. Por ejemplo, la ruta de acceso predeterminada en Windows 7 es `C:\ProgramData\VMware\VMware vSphere Auto Deploy\ssl`.
   - En vCenter Server Appliance, los archivos se encuentran en `/etc/vmware-rbd/ssl/`.

   De manera predeterminada, vCenter Server 6.0 y las versiones posteriores utilizan VMware Certificate Authority (VMCA).

Resultados

Al iniciar un host configurado para vSphere Auto Deploy, el host se comunica con el servidor DHCP y, a continuación, es dirigido al servidor vSphere Auto Deploy, el cual aprovisiona el host con el perfil de imagen que se especificó en el conjunto de reglas activo.

Pasos siguientes

- Defina una regla para asignar un perfil de imagen y un perfil de host opcional, una ubicación de host o un paquete de scripts al host. Para administrar vSphere Auto Deploy con cmdlets de PowerCLI, consulte la sección Administrar vSphere Auto Deploy con cmdlets de PowerCLI. Para administrar vSphere Auto Deploy con vSphere Web Client, consulte la sección Administrar vSphere Auto Deploy con vSphere Web Client.
- (opcional) Configure el primer host que aprovisione como un host de referencia. Utilice el almacenamiento y la red, entre otras opciones que desea que el host de destino comparta. Cree un perfil de host para el host de referencia y escriba una regla que asigne tanto el perfil de imagen que ya se ha probado como el perfil de host a los hosts de destino.
- (opcional) Si desea que vSphere Auto Deploy sobrescriba las particiones existentes, configure un host de referencia de manera que realice la partición de forma automática y, a continuación, aplique el perfil de host del host de referencia a otros hosts. Consulte Configurar un host de referencia para la creación automática de particiones .
- (opcional) Si debe configurar información específica de un host, configure el perfil de host del host de referencia de manera que solicite la interacción del usuario. Para obtener más información sobre la personalización de host, consulte la documentación *Perfiles de host de vSphere*.

Usar los cmdlets de vSphere Auto Deploy

Los cmdlets de vSphere Auto Deploy se implementan como cmdlets de Microsoft PowerShell y se incluyen en PowerCLI. Los usuarios de los cmdlets de vSphere Auto Deploy pueden aprovechar todas las funciones de PowerCLI.

Los usuarios experimentados de PowerShell también pueden utilizar los cmdlets de vSphere Auto Deploy del mismo modo que los cmdlets de PowerShell. Si no está familiarizado con PowerShell y PowerCLI, las sugerencias siguientes pueden ser de utilidad.

Puede escribir cmdlets, parámetros y valores de parámetros en el shell de PowerCLI.

- Obtenga ayuda para cualquier cmdlet a través de `Get-Help`*`cmdlet_name`*.
- Recuerde que PowerShell no distingue mayúsculas de minúsculas.
- Utilice la opción de finalización con tabulación para los nombres de cmdlets y parámetros.
- Puede aplicar formato a cualquier resultado de cmdlet o variable mediante `Format-List` o `Format-Table`, o mediante sus formas abreviadas: `fl` o `ft`. Para obtener más información, ejecute el cmdlet `Get-Help Format-List`.

Transmitir parámetros por nombre

Puede transmitir parámetros por nombre en la mayoría de los casos y rodear los valores de parámetros que contienen espacios o caracteres especiales con comillas dobles.

```
Copy-DeployRule -DeployRule testrule -ReplaceItem MyNewProfile
```

La mayoría de los ejemplos de la documentación *Instalar y configurar vSphere* transmiten parámetros por nombre.

Transmitir parámetros como objetos

Puede transmitir parámetros como objetos si desea ejecutar scripts y automatización. Transmitir parámetros como objetos resulta útil con los cmdlets que devuelven varios objetos y con los cmdlets que devuelven un solo objeto. Tenga en cuenta el ejemplo siguiente:

1 Vincule a una variable el objeto que contiene la información de cumplimiento de normas de un conjunto de reglas para un host.

   ```
   $tr = Test-DeployRuleSetCompliance MyEsxi42
   ```

2 Vea la propiedad `itemlist` del objeto para determinar la diferencia entre lo que contiene el conjunto de reglas y lo que usa el host actualmente.

   ```
   $tr.itemlist
   ```

3 Corrija el host para que use el conjunto de reglas modificado, utilizando el cmdlet `Repair-DeployRuleSetCompliance` con la variable.

   ```
   Repair-DeployRuleSetCompliance $tr
   ```

En este ejemplo, se corrige el host la próxima vez que se arranca.

Configurar licencias masivas

Puede utilizar vSphere Web Client o ESXi Shell para especificar claves de licencia individuales o configurar licencias masivas mediante los cmdlets de PowerCLI. Las licencias masivas funcionan

para todos los hosts ESXi, pero son especialmente útiles para los hosts aprovisionados con vSphere Auto Deploy.

La asignación de claves de licencia mediante vSphere Web Client y la asignación de licencias mediante los cmdlets de PowerCLI funcionan de manera diferente.

Asignación de claves de licencia mediante vSphere Web Client

Puede asignar claves de licencia a un host al agregar el host al sistema vCenter Server o cuando un sistema vCenter Server administra el host.

Asignar claves de licencia mediante LicenseDataManager PowerCLI

Puede especificar un conjunto de claves de licencia para agregar a un conjunto de hosts. Las claves de licencia se agregan a la base de datos de vCenter Server. Cada vez que se agrega un host al sistema vCenter Server o vuelve a conectarse a él, se le asigna una clave de licencia. Una clave de licencia que se asigna mediante PowerCLI se trata como una clave de licencia predeterminada. Cuando se agrega o se vuelve a conectar un host sin licencia, se le asigna la clave de licencia predeterminada. Si un host ya tiene licencia, mantiene su clave de licencia.

En el ejemplo siguiente, se asignan licencias a todos los hosts de un centro de datos. También puede asociar licencias con hosts y clústeres.

El ejemplo siguiente está destinado a usuarios avanzados de PowerCLI que saben cómo usar variables de PowerShell.

Requisitos previos

Preparar el sistema para vSphere Auto Deploy.

Procedimiento

1 En una sesión de PowerCLI, conéctese al sistema vCenter Server que desea utilizar y vincule el administrador de licencias asociado a una variable.

```
            Connect-VIServer -Server 192.XXX.X.XX -User username -Password password
$licenseDataManager = Get-LicenseDataManager
```

2 Ejecute un cmdlet que recupere el centro de datos en el que se encuentran los hosts para los cuales desea utilizar la característica de licencias masivas.

```
$hostContainer = Get-Datacenter -Name Datacenter-X
```

También puede ejecutar un cmdlet que recupere un clúster con la finalidad de utilizar licencias masivas para todos los hosts de un clúster, o que recupere una carpeta con la finalidad de utilizar licencias masivas para todos los hosts de una carpeta.

3 Cree un nuevo objeto `LicenseData` y un objeto `LicenseKeyEntry` con la clave de licencia y el identificador de tipo asociados.

```
            $licenseData = New-Object VMware.VimAutomation.License.Types.LicenseData
$licenseKeyEntry = New-Object Vmware.VimAutomation.License.Types.LicenseKeyEntry
$licenseKeyEntry.TypeId = "vmware-vsphere" $licenseKeyEntry.LicenseKey = "XXXXX-XXXXX-
XXXXX-XXXXX-XXXXX"
```

4 Asocie el atributo `LicenseKeys` del objeto `LicenseData` que creó en el paso 3 con el objeto `LicenseKeyEntry`.

`$licenseData.LicenseKeys += $licenseKeyEntry`

5 Actualice los datos de licencias del centro de datos con el objeto `LicenseData` y compruebe que la licencia esté asociada con el contenedor de host.

```
            $licenseDataManager.UpdateAssociatedLicenseData($hostContainer.Uid,
$licenseData) $licenseDataManager.QueryAssociatedLicenseData($hostContainer.Uid)
```

6 Aprovisione un host o más con vSphere Auto Deploy y asígnelos al centro de datos o al clúster al que asignó los datos de licencias.

7 Puede usar vSphere Web Client para verificar que el host se haya asignado correctamente a la licencia predeterminada `XXXXX-XXXXX-XXXXX-XXXXX-XXXXX`.

Resultados

Todos los hosts que se hayan asignado al centro de datos ahora cuentan con licencia de manera automática.

Administrar vSphere Auto Deploy con cmdlets de PowerCLI

Puede administrar vSphere Auto Deploy con cmdlets de PowerCLI para crear reglas que asocien hosts con perfiles de imagen, perfiles de host, scripts personalizados y ubicaciones en la instancia de vCenter Server de destino. También es posible actualizar los hosts mediante la comprobación del cumplimiento de normas y la corrección de los problemas de cumplimiento de normas que correspondan.

Descripción general de cmdlets de vSphere Auto Deploy PowerCLI

El usuario especifica las reglas que asignan perfiles de imagen y perfiles de host a los hosts mediante un conjunto de cmdlets de PowerCLI que se incluyen en PowerCLI.

Si no está familiarizado con PowerCLI, lea la documentación de PowerCLI y consulte Usar los cmdlets de vSphere Auto Deploy. Puede obtener ayuda en relación con cualquier comando en la línea de comandos de PowerShell.

- Ayuda básica: `Get-Help`*cmdlet_name*

- Ayuda detallada: `Get-Help` *cmdlet_name*`-Detailed`

Nota Al ejecutar cmdlets de vSphere Auto Deploy, proporcione todos los parámetros en la línea de comandos cuando invoque el cmdlet. No se recomienda proporcionar parámetros en modo interactivo.

Tabla 2-16. Cmdlets de PowerCLI del motor de reglas

Comando	Descripción
`Get-DeployCommand`	Devuelve una lista de cmdlets de vSphere Auto Deploy.
`New-DeployRule`	Crea una nueva regla con los elementos y los patrones especificados.
`Set-DeployRule`	Actualiza una regla existente con los elementos y los patrones especificados. No es posible actualizar una regla que forma parte de un conjunto de reglas.
`Get-DeployRule`	Recupera las reglas con los nombres especificados.
`Copy-DeployRule`	Clona y actualiza una regla existente.
`Add-DeployRule`	Agrega una regla o más al conjunto de reglas de trabajo y, de forma predeterminada, también al conjunto de reglas activo. Utilice el parámetro `NoActivate` para agregar una regla solamente al conjunto de reglas de trabajo.
`Remove-DeployRule`	Elimina una regla o más del conjunto de reglas de trabajo y del conjunto de reglas activo. Ejecute este comando con el parámetro `-Delete` para eliminar la regla por completo.
`Set-DeployRuleset`	Establece de manera explícita la lista de reglas en el conjunto de reglas de trabajo.
`Get-DeployRuleset`	Recupera el conjunto de reglas de trabajo o el conjunto de reglas activo actuales.
`Switch-ActiveDeployRuleset`	Activa un conjunto de reglas para que todas las solicitudes nuevas se evalúen mediante el conjunto de reglas.
`Get-VMHostMatchingRules`	Recupera las reglas que coinciden con un patrón. Por ejemplo, es posible recuperar todas las reglas que se aplican a un host o a varios. Utilice este cmdlet principalmente para depuración.
`Test-DeployRulesetCompliance`	Comprueba si los elementos asociados con un host especificado cumplen los criterios del conjunto de reglas activo.
`Repair-DeployRulesetCompliance`	En función del resultado de `Test-DeployRulesetCompliance`, este cmdlet actualiza el perfil de imagen, el perfil de host y la ubicación de cada host en el inventario de vCenter Server. El cmdlet puede aplicar perfiles de imagen, aplicar perfiles de host o transferir hosts a carpetas o clústeres especificados previamente en el sistema vCenter Server.
`Apply-EsxImageProfile`	Asocia el perfil de imagen especificado con el host especificado.

Tabla 2-16. Cmdlets de PowerCLI del motor de reglas (continuación)

Comando	Descripción
`Get-VMHostImageProfile`	Recupera el perfil de imagen que utiliza un host especificado. Este cmdlet es diferente al cmdlet `Get-EsxImageProfile` en vSphere ESXi Image Builder.
`Repair-DeployImageCache`	Utilice este cmdlet solamente si la memoria caché de imagen de vSphere Auto Deploy se elimina por accidente.
`Get-VMHostAttributes`	Recupera los atributos de un host que se utilizan cuando el servidor vSphere Auto Deploy evalúa las reglas.
`Get-DeployMachineIdentity`	Devuelve un valor de cadena que vSphere Auto Deploy utiliza para vincular forma lógica un host ESXi de vCenter Server con una máquina física.
`Set-DeployMachineIdentity`	Vincula de forma lógica un objeto de host en la base de datos de vCenter Server con una máquina física. Utilice este cmdlet para agregar hosts sin especificar reglas.
`Get-DeployOption`	Recupera las opciones de configuración globales de vSphere Auto Deploy. Actualmente, este cmdlet es compatible con la opción `vlan-id`, la cual especifica el identificador de VLAN predeterminado para la red de administración de ESXi de un host aprovisionado con vSphere Auto Deploy. vSphere Auto Deploy utiliza el valor solo si el host se arranca sin un perfil de host.
`Set-DeployOption`	Establece el valor de una opción de configuración global. Actualmente, es compatible con la opción `vlan-id` para establecer un identificador de la VLAN predeterminado para la red de administración de ESXi.
`Add-ProxyServer`	Agrega un servidor proxy a la base de datos de vSphere Auto Deploy. Ejecute el comando con el parámetro `-Address` para especificar la dirección IPv4 o IPv6. La dirección puede incluir un número de puerto.
`List-ProxyServer`	Lista los servidores proxy que están registrados actualmente en vSphere Auto Deploy.
`Delete-ProxyServer`	Elimina uno o varios servidores proxy de la lista de los servidores proxy registrados en vSphere Auto Deploy. Puede ejecutar el comando con el parámetro `-id` desde la lista de servidores proxy o con el parámetro `-Address` especificando la dirección IPv4 o IPv6 del servidor proxy que desea eliminar.
`Add-ScriptBundle`	Agrega uno o varios paquetes de scripts al servidor vSphere Auto Deploy.
`Get-ScriptBundle`	Recupera la lista de paquetes de scripts disponible en el servidor vSphere Auto Deploy, así como los scripts que contiene.

Asignar un perfil de imagen a hosts

Antes de que pueda aprovisionar un host, deberá crear reglas que asignen un perfil de imagen a cada host que desee aprovisionar con vSphere Auto Deploy.

Las reglas de extensibilidad de vSphere Auto Deploy obligan a que los VIB en el nivel CommunitySupported solo puedan contener archivos de determinadas ubicaciones predefinidas, como la ruta de complementos de ESXCLI, la ruta de complementos de jumpstart, etc. Si agrega un VIB que se encuentra en una ubicación diferente de la de un perfil de imagen, aparecerá una advertencia. Puede anular la advertencia utilizando la opción `force` (forzar).

Si realiza una llamada al cmdlet `New-DeployRule` en un perfil de imagen que incluye VIB en el nivel CommunitySupported que infrinja la regla, establezca `$DeployNoSignatureCheck = $true` antes de agregar el perfil de imagen. Con esta configuración, el sistema omitirá la validación de firma y no realizará la comprobación de reglas de extensibilidad.

Nota Los perfiles de imagen que incluyen VIB en el nivel CommunitySupported no se admiten en los sistemas de producción.

Requisitos previos

- Prepare el sistema para vSphere Auto Deploy. Para obtener más información, consulte *Instalación y configuración de vSphere*.

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Connect-VIServer` para conectarse al sistema vCenter Server con el que se registró vSphere Auto Deploy.

```
Connect-VIServer ipv4_or_ipv6_address
```

Es posible que el cmdlet devuelva una advertencia de certificado de servidor. En un entorno de producción, asegúrese de que no se emita ninguna advertencia de certificado de servidor. En un entorno de desarrollo, puede omitir la advertencia.

2 Determine la ubicación del almacén de software público o defina un perfil de imagen personalizado con vSphere ESXi Image Builder.

3 Ejecute `Add-EsxSoftwareDepot` para agregar el almacén de software que contiene el perfil de imagen a la sesión de PowerCLI.

Tipo de almacén	Cmdlet
Almacén remoto	Ejecute **`Add-EsxSoftwareDepot`** ***`depot_url`***.
Archivo ZIP	a Descargue el archivo ZIP en la ruta de acceso de archivo local. b Ejecute **`Add-EsxSoftwareDepot`** **`C:\`*****`file_path`*****`\`*****`my_offline_depot`*****`.zip`**.

4 En el almacén, busque el perfil de imagen que desea utilizar ejecutando el cmdlet `Get-EsxImageProfile`.

   De manera predeterminada, el almacén de ESXi incluye un perfil de imagen base que incluye VMware Tools y tiene la cadena `standard` en su nombre y un perfil de imagen base que no incluye VMware Tools.

5 Defina una regla en la que los hosts con determinados atributos, por ejemplo un rango de direcciones IP, estén asignados al perfil de imagen.

   ```
   New-DeployRule -Name "testrule" -Item "My Profile25" -Pattern "vendor=Acme,Zven",
   "ipv4=192.XXX.1.10-192.XXX.1.20"
   ```

   Si un nombre contiene espacios, se requieren comillas dobles. De lo contrario, es opcional. Especifique `-AllHosts` en lugar de un patrón para aplicar el elemento a todos los hosts.

   El cmdlet crea una regla con el nombre `testrule`. La regla asigna el perfil de imagen con el nombre My Profile25 a todos los hosts con un proveedor de Acme o Zven que también tienen una dirección IP en el rango especificado.

6 Agregue la regla al conjunto de reglas.

   ```
   Add-DeployRule testrule
   ```

   De manera predeterminada, la regla se agrega al conjunto de reglas en funcionamiento y al conjunto de reglas activo. Si utiliza el parámetro `NoActivate`, el conjunto de reglas en funcionamiento no se convierte en el conjunto de reglas activo.

Resultados

Cuando el host arranca desde iPXE, informa de los atributos de la máquina a la consola. Utilice el mismo formato de los atributos al escribir reglas de implementación.

```
******************************************************************
* Booting through VMware AutoDeploy...
*
* Machine attributes:
* . asset=No Asset Tag
* . domain=vmware.com
* . hostname=myhost.mycompany.com
* . ipv4=XX.XX.XXX.XXX
* . mac=XX:Xa:Xb:Xc:Xx:XX
* . model=MyVendorModel
* . oemstring=Product ID: XXXXXX-XXX
* . serial=XX XX XX XX XX XX...
* . uuid=XXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXX
* . vendor=MyVendor
******************************************************************
```

Pasos siguientes

- Para los hosts que ya se han aprovisionado con vSphere Auto Deploy, realice la prueba de cumplimiento de normas y las operaciones de reparación con la finalidad de aprovisionarlos con el nuevo perfil de imagen. Consulte Probar y reparar cumplimiento de reglas .
- Encienda los hosts no aprovisionados para aprovisionarlos con el nuevo perfil de imagen.

Escribir una regla y asignar un perfil de host a hosts

vSphere Auto Deploy puede asignar un perfil de host a uno o más hosts. El perfil de host puede incluir información sobre la configuración de almacenamiento, la configuración de red u otras características del host. Si agrega un host a un clúster, se utiliza el perfil de host de ese clúster.

En muchos casos, puede asignar un host a un clúster en lugar de especificar un perfil de host explícitamente. El host utiliza el perfil de host del clúster.

Requisitos previos

- Instale PowerCLI y todo el software de requisito previo. Para obtener información, consulte *Instalar y configurar vSphere*.
- Exporte el perfil de host que desea utilizar.

Procedimiento

1. En una sesión de PowerCLI, ejecute el cmdlet `Connect-VIServer` para conectarse al sistema vCenter Server con el que se registró vSphere Auto Deploy.

   ```
   Connect-VIServer ipv4_or_ipv6_address
   ```

   Es posible que el cmdlet devuelva una advertencia de certificado de servidor. En un entorno de producción, asegúrese de que no se emita ninguna advertencia de certificado de servidor. En un entorno de desarrollo, puede omitir la advertencia.

2. Con vSphere Web Client, configure un host con los parámetros que desee usar y cree un perfil de host a partir de él.

3. Busque el nombre del perfil de host mediante la ejecución del cmdlet `Get-VMhostProfile` de PowerCLI, pasando el host ESXi a partir del cual creó un perfil de host.

4. En el símbolo de PowerCLI, defina una regla en la que los perfiles de host se asignen a hosts con ciertos atributos; por ejemplo, un intervalo de direcciones IP.

   ```
   New-DeployRule -Name "testrule2" -Item my_host_profile -Pattern "vendor=Acme,Zven",
   "ipv4=192.XXX.1.10-192.XXX.1.20"
   ```

   El elemento especificado se asigna a todos los hosts que posean los atributos especificados. Este ejemplo especifica una regla denominada testrule2. Esta asigna el perfil de host especificado *my_host_profile* a todos los hosts que tengan una dirección IP dentro del intervalo especificado y cuyo fabricante sea Acme o Zven.

5 Agregue la regla al conjunto de reglas.

```
Add-DeployRule testrule2
```

De forma predeterminada, el conjunto de reglas en funcionamiento se convierte en el conjunto de reglas activo y los cambios en él se vuelven activos cuando agrega una regla. Si utiliza el parámetro `NoActivate`, el conjunto de reglas en funcionamiento no se convierte en el conjunto de reglas activo.

Pasos siguientes

- Asigne un host ya aprovisionado con vSphere Auto Deploy al nuevo perfil de host. Para ello, realice operaciones de prueba de cumplimiento y reparación en esos hosts. Para obtener más información, consulte Probar y reparar cumplimiento de reglas .
- Encienda los hosts no aprovisionados para aprovisionarlos con el perfil de host.

Escribir una regla y asignar un host a una carpeta o un clúster

vSphere Auto Deploy puede asignar un host a una carpeta o un clúster. Cuando el host arranca, vSphere Auto Deploy lo agrega a la ubicación que se especifica en vCenter Server. El host asignado a un clúster hereda el perfil de host del clúster.

Requisitos previos

- Preparar el sistema para vSphere Auto Deploy
- Compruebe que la carpeta seleccionada esté en un centro de datos o clúster. No puede asignar el host a una carpeta de nivel superior independiente.

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Connect-VIServer` para conectarse al sistema vCenter Server con el que se registró vSphere Auto Deploy.

```
Connect-VIServer ipv4_or_ipv6_address
```

Es posible que el cmdlet devuelva una advertencia de certificado de servidor. En un entorno de producción, asegúrese de que no se emita ninguna advertencia de certificado de servidor. En un entorno de desarrollo, puede omitir la advertencia.

2 Defina una regla en la que los hosts con ciertos atributos, por ejemplo, un rango de direcciones IP, se asignan a una carpeta o un clúster.

```
New-DeployRule -Name testrule3 -Item "my folder"    -Pattern "vendor=Acme,Zven",
"ipv4=192.XXX.1.10-192.XXX.1.20"
```

Este ejemplo pasa la carpeta por el nombre. En cambio, puede pasar una carpeta, un clúster o un objeto de centro de datos que recupere con el comando cmdlet `Get-Folder`, `Get-Cluster` o `Get-Datacenter`.

3 Agregue la regla al conjunto de reglas.

```
Add-DeployRule testrule3
```

De forma predeterminada, el conjunto de reglas en funcionamiento se convierte en el conjunto de reglas activo y los cambios en él se vuelven activos cuando agrega una regla. Si utiliza el parámetro `NoActivate`, el conjunto de reglas en funcionamiento no se convierte en el conjunto de reglas activo.

Pasos siguientes

- Para asignar un host ya aprovisionado con vSphere Auto Deploy a la nueva ubicación de carpeta o clúster, realice una operación de cumplimiento de prueba y reparación. Consulte Probar y reparar cumplimiento de reglas .
- Encienda los hosts no aprovisionados para agregarlos a la ubicación especificada de vCenter Server.

Configurar un sistema sin estado mediante la ejecución de un script personalizado

Puede utilizar vSphere Auto Deploy para configurar uno o varios hosts asociando scripts personalizados con una regla de vSphere Auto Deploy.

Los scripts se ejecutan en orden alfabético después del flujo de trabajo de arranque de ESXi del host.inicial del host.

Requisitos previos

- Prepare el sistema para vSphere Auto Deploy. Para obtener más información, consulte *Instalación y configuración de vSphere*.
- Compruebe que el paquete de scripts que desea asociar a la regla de vSphere Auto Deploy tiene el formato `.tgz` y un tamaño máximo de 10 MB, y que está escrito en lenguaje de script de ash de BusyBox o Python.

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Connect-VIServer` para conectarse al sistema vCenter Server con el que se registró vSphere Auto Deploy.

```
Connect-VIServer ipv4_or_ipv6_address
```

Es posible que el cmdlet devuelva una advertencia de certificado de servidor. En un entorno de producción, asegúrese de que no se emita ninguna advertencia de certificado de servidor. En un entorno de desarrollo, puede omitir la advertencia.

2 Ejecute el cmdlet `Add-ScriptBundle` para agregar el paquete de scripts que contiene los scripts necesarios al inventario de vSphere Auto Deploy.

```
Add-ScriptBundle c:/temp/MyScriptBundle.tgz
```

El nombre del paquete de scripts sin la extensión `.tgz` es el identificador del nombre o el objeto del elemento del paquete de scripts. Puede actualizar el paquete de scripts existente utilizando el parámetro `-Update` con el cmdlet `Add-ScriptBundle`.

3 (opcional) Ejecute el cmdlet `Get-ScriptBundle` para comprobar que el paquete de scripts se agregó al inventario de vSphere Auto Deploy.

4 Defina una regla en la que los hosts con determinados atributos, por ejemplo un rango de direcciones IP, estén asignados al paquete de scripts.

```
New-DeployRule -Name "testrule4" -Item "MyScriptBundle" -Pattern "vendor=Acme,Zven",
"ipv4=192.XXX.1.10-192.XXX.1.20"
```

Si un nombre contiene espacios, se requieren comillas dobles. De lo contrario, es opcional. Especifique `-AllHosts` en lugar de un patrón para aplicar el elemento a todos los hosts.

Cree una regla denominada *testrule4*. La regla asigna el paquete de scripts con el nombre My Script Bundle a todos los hosts con un proveedor de Acme o Zven que también tienen una dirección IP en el rango especificado. Puede utilizar el identificador de nombre del paquete de scripts o el objeto que devuelve el cmdlet `Get-ScriptBundle` para identificar el paquete de scripts que quiere asociar a la regla.

5 Agregue la regla al conjunto de reglas.

```
Add-DeployRule testrule4
```

De manera predeterminada, la regla se agrega al conjunto de reglas en funcionamiento y al conjunto de reglas activo. Si utiliza el parámetro `NoActivate`, el conjunto de reglas en funcionamiento no se convierte en el conjunto de reglas activo.

Pasos siguientes

- Para los hosts que ya se han aprovisionado con vSphere Auto Deploy, realice la prueba de cumplimiento de normas y las operaciones de reparación con la finalidad de aprovisionarlos con los nuevos scripts. Consulte Probar y reparar cumplimiento de reglas .
- Encienda los hosts no aprovisionados para aprovisionarlos con los nuevos scripts.

Probar y reparar cumplimiento de reglas

Cuando se agrega una regla al conjunto de reglas de vSphere Auto Deploy o cuando se realizan cambios en una regla o más, los hosts no se actualizan de manera automática. vSphere Auto Deploy aplica las reglas nuevas únicamente cuando se prueba el cumplimiento de reglas y se realizan las correcciones pertinentes.

Requisitos previos

- Prepare el sistema para vSphere Auto Deploy. Para obtener más información, consulte *Instalación y configuración de vSphere*.

- Compruebe que la infraestructura incluya un host ESXi o más aprovisionados con vSphere Auto Deploy y que el host en el que se instaló PowerCLI pueda acceder a esos hosts ESXi.

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Connect-VIServer` para conectarse al sistema vCenter Server con el que se registró vSphere Auto Deploy.

```
Connect-VIServer ipv4_or_ipv6_address
```

Es posible que el cmdlet devuelva una advertencia de certificado de servidor. En un entorno de producción, asegúrese de que no se emita ninguna advertencia de certificado de servidor. En un entorno de desarrollo, puede omitir la advertencia.

2 Use PowerCLI para comprobar qué reglas de vSphere Auto Deploy están disponibles actualmente.

```
Get-DeployRule
```

El sistema devuelve las reglas y los patrones, y los elementos asociados.

3 Realice un cambio en una de las reglas disponibles.

Por ejemplo, puede cambiar el perfil de imagen y el nombre de la regla.

```
Copy-DeployRule -DeployRule testrule -ReplaceItem MyNewProfile
```

No se puede editar una regla que ya se agregó a un conjunto de reglas activo. En lugar de ello, puede copiar la regla y reemplazar el elemento o el patrón que desea cambiar.

4 Compruebe que pueda acceder al host para el cual desea probar el cumplimiento del conjunto de reglas.

```
Get-VMHost -Name MyEsxi42
```

5 Ejecute el cmdlet que prueba el cumplimiento del conjunto de reglas para el host y vincule el valor devuelto a una variable para usarlo en otro momento.

```
$tr = Test-DeployRuleSetCompliance MyEsxi42
```

6 Examine las diferencias entre el contenido del conjunto de reglas y la configuración del host.

```
$tr.itemlist
```

El sistema devolverá una tabla de elementos actuales y esperados si el host en el que se desea probar el cumplimiento de un nuevo conjunto de reglas cumple con el conjunto de reglas activo.

```
CurrentItem                           ExpectedItem
-----------                           ------------
My Profile 25MyNewProfile
```

7 Corrija el host para que use el conjunto de reglas modificado la próxima vez que arranque.

```
Repair-DeployRuleSetCompliance $tr
```

Pasos siguientes

Si la regla que modificó ha especificado la ubicación en el inventario, el cambio se aplica cuando se corrigen los problemas de cumplimiento. Para todos los demás cambios, reinicie el host para que vSphere Auto Deploy aplique la nueva regla y logre el cumplimiento entre el conjunto de reglas y el host.

Registrar la dirección de un servidor proxy de almacenamiento en caché con vSphere Auto Deploy

El arranque simultáneo de un gran número de hosts sin estado supone una carga considerable para el servidor vSphere Auto Deploy. Puede equilibrar la carga de las solicitudes entre el servidor vSphere Auto Deploy y uno o varios servidores proxy más que registre en vSphere Auto Deploy.

Requisitos previos

- Prepare el sistema para vSphere Auto Deploy. Para obtener más información, consulte *Instalación y configuración de vSphere*.

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Connect-VIServer` para conectarse al sistema vCenter Server con el que se registró vSphere Auto Deploy.

```
Connect-VIServer ipv4_or_ipv6_address
```

Es posible que el cmdlet devuelva una advertencia de certificado de servidor. En un entorno de producción, asegúrese de que no se emita ninguna advertencia de certificado de servidor. En un entorno de desarrollo, puede omitir la advertencia.

2 Registre direcciones de un servidor proxy de almacenamiento en caché en vSphere Auto Deploy ejecutando el cmdlet `Add-ProxyServer`.

```
Add-ProxyServer -Address 'https://proxy_server_ip_address:port_number'
```

Puede ejecutar el cmdlet varias veces para registrar varios servidores proxy. La dirección puede incluir un número de puerto.

3 (opcional) Ejecute el cmdlet `List-ProxyServer` para verificar que el servidor proxy de almacenamiento en caché está registrado en vSphere Auto Deploy.

Administrar vSphere Auto Deploy con vSphere Web Client

Puede agregar hosts de ESXi al inventario de vSphere Auto Deploy y crear, supervisar y administrar las reglas de vSphere Auto Deploy y las asociaciones de hosts ESXi usando vSphere Web Client.

Crear una regla de implementación

Antes de aprovisionar los hosts ESXi con vSphere Auto Deploy, debe crear reglas que asignen perfiles de imagen, perfiles de host y ubicaciones de host a los hosts. Un host ESXi puede coincidir con más de un criterio de regla de vSphere Auto Deploy; si eso sucede, se tiene en cuenta el orden de las reglas.

Requisitos previos

- Prepare el sistema e instale el servidor Auto Deploy. Para obtener más información, consulte Preparar el sistema para vSphere Auto Deploy.
- Si desea incluir un perfil de imagen en la regla, compruebe que se haya agregado el almacén de software necesario al inventario. Consulte Agregar un almacén de software o Importar un almacén de software.

Procedimiento

1 Iniciar el asistente Nueva regla de implementación

   Puede crear una nueva regla de vSphere Auto Deploy usando el asistente **Nueva regla de implementación**.

2 Asignar nombre a la regla y definir criterios de coincidencia en el asistente Nueva regla de implementación

   Al iniciar el asistente **Nueva regla de implementación**, primero debe introducir un nombre de regla y seleccionar un patrón para aplicar la regla a algunos o todos los hosts del inventario.

3 Seleccionar un perfil de imagen en el asistente Nueva regla de implementación

   En el asistente **Nueva regla de implementación**, tiene la opción de asignar un perfil de imagen a los hosts que coincidan con los criterios de la regla.

4 Seleccionar un perfil de host en el asistente Nueva regla de implementación

   En el asistente **Nueva regla de implementación**, tiene la opción de asignar un perfil de host a los hosts que coincidan con los criterios de la regla.

5 Seleccionar la ubicación del host en el asistente Nueva regla de implementación

   En el asistente **Nueva regla de implementación**, puede agregar los hosts que coincidan con el criterio de la regla a una ubicación específica.

6 Ver el resumen del asistente Nueva regla de implementación

En el asistente **Nueva regla de implementación**, puede recuperar la configuración de la nueva regla de vSphere Auto Deploy antes de completar el asistente.

Pasos siguientes

- Active una regla de vSphere Auto Deploy. Consulte Activar, desactivar y reordenar las reglas de implementación.
- Edite una regla de vSphere Auto Deploy. Consulte Editar una regla de implementación.
- Vea las asociaciones de perfil de imagen, perfil de host y ubicación de un host. Consulte Ver asociaciones de hosts.
- Corrija los hosts que no cumplan con las reglas. Consulte Corregir un host no compatible.
- Cambie la asociación de perfil de imagen de un host. Consulte Editar la asociación de perfil de imagen de un host.

Iniciar el asistente Nueva regla de implementación

Puede crear una nueva regla de vSphere Auto Deploy usando el asistente **Nueva regla de implementación**.

Procedimiento

1 En la página de inicio de vSphere Web Client, haga clic en **Auto Deploy**.

De manera predeterminada, solo la función de administrador incluye privilegios para usar el servicio de vSphere Auto Deploy.

2 En la pestaña **Reglas de implementación**, haga clic en **Nueva regla de implementación**.

Resultados

Aparece el asistente **Nueva regla de implementación**.

Asignar nombre a la regla y definir criterios de coincidencia en el asistente Nueva regla de implementación

Al iniciar el asistente **Nueva regla de implementación**, primero debe introducir un nombre de regla y seleccionar un patrón para aplicar la regla a algunos o todos los hosts del inventario.

Procedimiento

1 En la página de nombre y hosts del asistente, escriba un nombre para la nueva regla.

2 Seleccione un patrón para aplicar la regla a los hosts del inventario.

Puede optar por aplicar la regla a todos los hosts del inventario, o bien aplicarla solo a los hosts que coincidan con un patrón específico. Puede seleccionar uno o varios patrones.

Por ejemplo, la regla se puede aplicar solo a los hosts de un dominio de vCenter Single Sign-On con un nombre de host específico o a los hosts que coincidan con un rango de IPv4 específico.

3 Haga clic en **Siguiente**.

Seleccionar un perfil de imagen en el asistente Nueva regla de implementación

En el asistente **Nueva regla de implementación**, tiene la opción de asignar un perfil de imagen a los hosts que coincidan con los criterios de la regla.

Requisitos previos

Si desea incluir un perfil de imagen en la regla, compruebe que se haya agregado el almacén de software necesario al inventario. Consulte Agregar un almacén de software o Importar un almacén de software.

Procedimiento

1 En la página Seleccionar perfil de imagen del asistente, seleccione un perfil de imagen.

Opción	Acción
Si no desea asignar un perfil de imagen a los hosts seleccionados	Active la casilla **Sin perfil de imagen**.
Si desea asignar un perfil de imagen a los hosts seleccionados	1 Seleccione un almacén de software en el menú desplegable. 2 Seleccione un perfil de imagen de la lista. 3 (Opcional) Si desea omitir la verificación de nivel de aceptación para el perfil de imagen, active la casilla **Omitir comprobación de firma de perfil de imagen**.

2 Haga clic en **Siguiente**.

Seleccionar un perfil de host en el asistente Nueva regla de implementación

En el asistente **Nueva regla de implementación**, tiene la opción de asignar un perfil de host a los hosts que coincidan con los criterios de la regla.

Procedimiento

1 En la página Seleccionar perfil de host del asistente, seleccione un perfil de host.

Opción	Acción
Si no desea asignar un perfil de host a los hosts seleccionados	Active la casilla **No incluir un perfil de host**.
Si desea asignar un perfil de host a los hosts seleccionados	Seleccione un perfil de host de la lista.

2 Haga clic en **Siguiente**.

Seleccionar la ubicación del host en el asistente Nueva regla de implementación

En el asistente **Nueva regla de implementación**, puede agregar los hosts que coincidan con el criterio de la regla a una ubicación específica.

Procedimiento

1 En la página para seleccionar la ubicación del host del asistente, seleccione una ubicación para los hosts que coincidan con la regla.

Opción	Acción
Si no desea seleccionar una ubicación de host	Active la casilla **No incluir una ubicación**.
Si desea seleccionar una ubicación específica para los hosts seleccionados	Seleccione un centro de datos, una carpeta o un clúster como ubicación de host.

2 Haga clic en **Siguiente**.

Ver el resumen del asistente Nueva regla de implementación

En el asistente **Nueva regla de implementación**, puede recuperar la configuración de la nueva regla de vSphere Auto Deploy antes de completar el asistente.

Procedimiento

1 En la página Listo para finalizar, revise la información de resumen para la nueva regla.

2 Haga clic en **Finalizar**.

Resultados

Para ver la regla recién creada, consulte la lista de la pestaña **Reglas de implementación**.

Clonar una regla de implementación

Puede usar una regla de vSphere Auto Deploy como plantilla y modificar solo partes de la regla en lugar de crear una nueva.

Requisitos previos

- Prepare el sistema e instale el servidor Auto Deploy. Para obtener más información, consulte Preparar el sistema para vSphere Auto Deploy.
- Cree una regla de vSphere Auto Deploy. Consulte Crear una regla de implementación.
- Si desea incluir un perfil de imagen en la regla, compruebe que se haya agregado el almacén de software necesario al inventario. Consulte Agregar un almacén de software o Importar un almacén de software.

Procedimiento

1 Iniciar el asistente Clonar regla de implementación

Puede clonar una regla de vSphere Auto Deploy existente usando el asistente **Clonar regla de implementación**.

2 Asignar nombre a la regla y definir criterios de coincidencia en el asistente Clonar regla de implementación

Al iniciar el asistente **Clonar regla de implementación** con el fin de clonar una regla de vSphere Auto Deploy, primero debe elegir si quiere mantener el nombre predeterminado de la regla clonada y si quiere cambiar los criterios de coincidencia de la regla.

3 Seleccionar un perfil de imagen en el asistente Clonar regla de implementación

En el asistente **Clonar regla de implementación**, tiene la opción de asignar un perfil de imagen a los hosts que coincidan con los criterios de la regla o mantener el mismo perfil de imagen usado en la regla clonada.

4 Seleccionar un perfil de host en el asistente Clonar regla de implementación

En el asistente **Clonar regla de implementación**, tiene la opción de asignar un perfil de host a los hosts que coincidan con los criterios de la regla o mantener el mismo perfil de host usado en la regla clonada.

5 Seleccionar la ubicación del host en Clonar regla de implementación

En el asistente **Clonar regla implementación**, puede agregar los hosts que coincidan con el criterio de la regla a una ubicación específica o mantener la ubicación que la regla clonada utiliza.

6 Ver el resumen del asistente Clonar regla de implementación

Puede recuperar la configuración de la regla de vSphere Auto Deploy clonada antes de completar el asistente.

Pasos siguientes

- Active una regla de vSphere Auto Deploy. Consulte Activar, desactivar y reordenar las reglas de implementación.
- Edite una regla de vSphere Auto Deploy. Consulte Editar una regla de implementación.

Iniciar el asistente Clonar regla de implementación

Puede clonar una regla de vSphere Auto Deploy existente usando el asistente **Clonar regla de implementación**.

Procedimiento

1 En la página de inicio de vSphere Web Client, haga clic en **Auto Deploy**.

De manera predeterminada, solo la función de administrador incluye privilegios para usar el servicio de vSphere Auto Deploy.

2 En la pestaña **Reglas de implementación**, seleccione una regla de la lista.

3 Haga clic en el icono **Clonar**.

Resultados

Aparece el asistente **Clonar regla de implementación**.

Asignar nombre a la regla y definir criterios de coincidencia en el asistente Clonar regla de implementación

Al iniciar el asistente **Clonar regla de implementación** con el fin de clonar una regla de vSphere Auto Deploy, primero debe elegir si quiere mantener el nombre predeterminado de la regla clonada y si quiere cambiar los criterios de coincidencia de la regla.

Procedimiento

1 En la página de nombre y hosts del asistente, escriba un nombre para la nueva regla.

2 Seleccione un patrón para aplicar la regla a los hosts del inventario.

   Puede optar por aplicar la regla a todos los hosts del inventario, o bien aplicarla solo a los hosts que coincidan con un patrón específico. Puede seleccionar uno o varios patrones.

   Por ejemplo, la regla se puede aplicar solo a los hosts de un dominio de vCenter Single Sign-On con un nombre de host específico o a los hosts que coincidan con un rango de IPv4 específico.

3 Haga clic en **Siguiente**.

Seleccionar un perfil de imagen en el asistente Clonar regla de implementación

En el asistente **Clonar regla de implementación**, tiene la opción de asignar un perfil de imagen a los hosts que coincidan con los criterios de la regla o mantener el mismo perfil de imagen usado en la regla clonada.

Requisitos previos

Si desea incluir un perfil de imagen en la regla, compruebe que se haya agregado el almacén de software necesario al inventario. Consulte Agregar un almacén de software o Importar un almacén de software.

Procedimiento

1 En la página Seleccionar perfil de imagen del asistente, seleccione un perfil de imagen.

Opción	Acción
Si no desea cambiar el perfil de imagen	Seleccione la opción **Mismo perfil de imagen**.
Si no desea asignar un perfil de imagen a los hosts seleccionados	Seleccione la opción **Sin perfil de imagen**.
Si desea asignar un nuevo perfil de imagen a los hosts seleccionados	1 Seleccione la opción **Buscar perfil de imagen**. 2 Seleccione un almacén de software en el menú desplegable. 3 Seleccione un perfil de imagen de la lista. 4 (Opcional) Si desea omitir la verificación de nivel de aceptación para el perfil de imagen, active la casilla **Omitir comprobación de firma de perfil de imagen**.

2 Haga clic en **Siguiente**.

Seleccionar un perfil de host en el asistente Clonar regla de implementación

En el asistente **Clonar regla de implementación**, tiene la opción de asignar un perfil de host a los hosts que coincidan con los criterios de la regla o mantener el mismo perfil de host usado en la regla clonada.

Procedimiento

- En la página Seleccionar perfil de host del asistente, seleccione un perfil de host.

Opción	Acción
Si quiere mantener el perfil de host usado en la regla clonada	Haga clic en **Siguiente**.
Si no desea asignar un perfil de host a los hosts seleccionados	Active la casilla **No incluir un perfil de host** y haga clic en **Siguiente**.
Si desea asignar un perfil de host nuevo a los hosts seleccionados	Seleccione un perfil de host en la lista y haga clic en **Siguiente**.

Seleccionar la ubicación del host en Clonar regla de implementación

En el asistente **Clonar regla implementación**, puede agregar los hosts que coincidan con el criterio de la regla a una ubicación específica o mantener la ubicación que la regla clonada utiliza.

Procedimiento

1 En la página para seleccionar la ubicación del host del asistente, seleccione una ubicación para los hosts que coincidan con la regla.

Opción	Acción
Si desea mantener la ubicación del host usada en la regla clonada	Deje la ubicación predeterminada.
SI no desea que la regla incluya una ubicación de host	Active la casilla **No incluir un perfil de host**.
Si desea seleccionar una nueva ubicación para los hosts seleccionados	Seleccione un centro de datos, una carpeta o un clúster como ubicación de host.

2 Haga clic en **Siguiente**.

Ver el resumen del asistente Clonar regla de implementación

Puede recuperar la configuración de la regla de vSphere Auto Deploy clonada antes de completar el asistente.

Procedimiento

1 En la página Listo para finalizar, revise la información de resumen para la nueva regla.

2 Haga clic en **Finalizar**.

Resultados

Para ver la regla recién creada, consulte la lista de la pestaña **Reglas de implementación**.

Editar una regla de implementación

Es posible editar una regla de vSphere Auto Deploy solo si la regla está en estado inactivo en el inventario. Puede editar el nombre de la regla, los hosts coincidentes y el perfil de imagen, el perfil de host y la ubicación de host asignados.

- Editar el nombre y los hosts coincidentes de una regla

  Si una regla del inventario se encuentra en estado inactivo, puede editar su nombre y cambiar la selección de los hosts que coincidan con sus criterios.

- Editar una regla para asignar otro perfil de imagen a los hosts

  Si una regla del inventario se encuentra en estado inactivo, puede editarla y asignar otro perfil de imagen a los hosts que coincidan con ella.

- Editar una regla para asignar otro perfil de host a los hosts

  Si una regla del inventario se encuentra en estado inactivo, puede editarla y asignar otro perfil de host a los hosts que coincidan con sus criterios.

- Editar la ubicación de hosts de una regla

  Si una regla del inventario se encuentra en estado inactivo, puede editarla y asignar otra ubicación de host a los hosts que coincidan con sus criterios.

Editar el nombre y los hosts coincidentes de una regla

Si una regla del inventario se encuentra en estado inactivo, puede editar su nombre y cambiar la selección de los hosts que coincidan con sus criterios.

Requisitos previos

- Prepare el sistema e instale el servidor Auto Deploy. Para obtener más información, consulte Preparar el sistema para vSphere Auto Deploy.
- Cree una regla de vSphere Auto Deploy. Consulte Crear una regla de implementación.

Procedimiento

1. En la página de inicio de vSphere Web Client, haga clic en **Auto Deploy**.

   De manera predeterminada, solo la función de administrador incluye privilegios para usar el servicio de vSphere Auto Deploy.

2. En la pestaña **Reglas de implementación**, seleccione la regla que desea editar en la lista de reglas del inventario y haga clic en **Editar**.

   Se mostrará el cuadro de diálogo Editar regla de implementación.

3. Seleccione la página **Nombre y hosts** y escriba un nuevo nombre para la regla.
4. Seleccione un patrón para aplicar la regla a los hosts del inventario.

   Puede optar por aplicar la regla a todos los hosts del inventario, o bien aplicarla solo a los hosts que coincidan con un patrón específico. Puede seleccionar uno o varios patrones.

Por ejemplo, la regla se puede aplicar solo a los hosts de un dominio de vCenter Single Sign-On con un nombre de host específico o a los hosts que coincidan con un rango de IPv4 específico.

5 Haga clic en **Aceptar**.

Editar una regla para asignar otro perfil de imagen a los hosts

Si una regla del inventario se encuentra en estado inactivo, puede editarla y asignar otro perfil de imagen a los hosts que coincidan con ella.

Requisitos previos

- Prepare el sistema e instale el servidor Auto Deploy. Para obtener más información, consulte Preparar el sistema para vSphere Auto Deploy.
- Cree una regla de vSphere Auto Deploy. Consulte Crear una regla de implementación.

Procedimiento

1 En la página de inicio de vSphere Web Client, haga clic en **Auto Deploy**.

   De manera predeterminada, solo la función de administrador incluye privilegios para usar el servicio de vSphere Auto Deploy.

2 En la pestaña **Reglas de implementación**, seleccione la regla que desea editar en la lista de reglas del inventario y haga clic en **Editar**.

   Se mostrará el cuadro de diálogo Editar regla de implementación.

3 Seleccione la página **Seleccionar perfil de imagen** para asignar un perfil de imagen a los hosts que coincidan con los criterios de la regla.

Opción	Acción
Si no desea cambiar el perfil de imagen	Seleccione la opción **Mismo perfil de imagen**.
Si no desea asignar un perfil de imagen a los hosts seleccionados	Seleccione la opción **Sin perfil de imagen**.
Si desea asignar un nuevo perfil de imagen a los hosts seleccionados	1 Seleccione la opción **Buscar perfil de imagen**. 2 Seleccione un almacén de software en el menú desplegable. 3 Seleccione un perfil de imagen de la lista. 4 (Opcional) Si desea omitir la verificación de nivel de aceptación para el perfil de imagen, active la casilla **Omitir comprobación de firma de perfil de imagen**.

4 Haga clic en **Aceptar**.

Editar una regla para asignar otro perfil de host a los hosts

Si una regla del inventario se encuentra en estado inactivo, puede editarla y asignar otro perfil de host a los hosts que coincidan con sus criterios.

Requisitos previos

- Prepare el sistema e instale el servidor Auto Deploy. Para obtener más información, consulte Preparar el sistema para vSphere Auto Deploy.
- Cree una regla de vSphere Auto Deploy. Consulte Crear una regla de implementación.

Procedimiento

1 En la página de inicio de vSphere Web Client, haga clic en **Auto Deploy**.

  De manera predeterminada, solo la función de administrador incluye privilegios para usar el servicio de vSphere Auto Deploy.

2 En la pestaña **Reglas de implementación**, seleccione la regla que desea editar en la lista de reglas del inventario y haga clic en **Editar**.

  Se mostrará el cuadro de diálogo Editar regla de implementación.

3 Seleccione la página **Seleccionar perfil de host** y asigne un nuevo perfil a los hosts que coincidan con la regla.

Opción	Acción
Si no desea asignar un perfil de host a los hosts seleccionados	Active la casilla **No incluir un perfil de host**.
Si desea asignar un perfil de host a los hosts seleccionados	Seleccione un perfil de host de la lista.

4 Haga clic en **Aceptar**.

Editar la ubicación de hosts de una regla

Si una regla del inventario se encuentra en estado inactivo, puede editarla y asignar otra ubicación de host a los hosts que coincidan con sus criterios.

Requisitos previos

- Prepare el sistema e instale el servidor Auto Deploy. Para obtener más información, consulte Preparar el sistema para vSphere Auto Deploy.
- Cree una regla de vSphere Auto Deploy. Consulte Crear una regla de implementación.

Procedimiento

1 En la página de inicio de vSphere Web Client, haga clic en **Auto Deploy**.

  De manera predeterminada, solo la función de administrador incluye privilegios para usar el servicio de vSphere Auto Deploy.

2 En la pestaña **Reglas de implementación**, seleccione la regla que desea editar en la lista de reglas del inventario y haga clic en **Editar**.

  Se mostrará el cuadro de diálogo Editar regla de implementación.

3 Seleccione la página **Seleccionar ubicación de host** y elija una ubicación para los hosts que coincidan con la regla.

Opción	Acción
Si no desea seleccionar una ubicación de host	Active la casilla **No incluir una ubicación**.
Si desea seleccionar una ubicación específica para los hosts seleccionados	Seleccione un centro de datos, una carpeta o un clúster como ubicación de host.

4 Haga clic en **Aceptar**.

Activar, desactivar y reordenar las reglas de implementación

Después de crear una regla de vSphere Auto Deploy, la regla queda en estado inactivo. Debe activar la regla para que se aplique. Puede usar el asistente Activar y reordenar para activar y desactivar reglas y para cambiar su orden.

La lista superior de la página **Activar y reordenar** del asistente muestra las reglas del conjunto de reglas activo. La lista inferior muestra las reglas inactivas.

Requisitos previos

- Prepare el sistema e instale el servidor Auto Deploy. Para obtener más información, consulte Preparar el sistema para vSphere Auto Deploy.
- Cree una regla de vSphere Auto Deploy. Consulte Crear una regla de implementación.

Procedimiento

1 En la página de inicio de vSphere Web Client, haga clic en **Auto Deploy**.

   De manera predeterminada, solo la función de administrador incluye privilegios para usar el servicio de vSphere Auto Deploy.

2 En la pestaña **Reglas de implementación**, haga clic en **Activar/desactivar reglas**.

   Aparece el asistente Activar y reordenar.

3 (opcional) Si desea desactivar una regla activa, seleccione la regla de la lista de reglas activas y haga clic en el botón **Desactivar**.

4 En la lista de reglas inactivas, seleccione la regla que desea activar y haga clic en el botón **Activar**.

5 (opcional) Si desea reordenar las reglas de la lista de reglas activas, seleccione la regla que desea mover hacia arriba o hacia abajo en la lista, y haga clic en los iconos **Subir** o **Bajar** sobre la lista de reglas activas.

   Las reglas se ordenan por prioridad. Por ejemplo, si se aplican dos o más reglas al mismo host, pero se definen de manera que aprovisionarán el host con perfiles de imagen, perfiles de host y ubicaciones diferentes, la regla con la posición más alta de la lista se aplica al host.

6 (opcional) Si desea probar una regla inactiva antes de activarla, active la casilla **Probar reglas antes de activación** y haga clic en **Siguiente**.

   a En la página Seleccionar destinos de prueba del asistente, en la pestaña **Filtrar**, seleccione los hosts en los que desea probar la regla inactiva y haga clic en **Siguiente**.

      En la pestaña **Seleccionado**, solo se muestran los hosts seleccionados.

   b En la página Vista previa de resultados de la prueba del asistente, seleccione un host de la lista para ver el estado actual del host y los cambios que se esperan después de la activación de la regla.

      Si el host cumple con la regla, no es necesario corregir el host tras activar la regla.

   c (opcional) Si desea corregir los hosts seleccionados después de la activación de la regla, active la casilla **Corregir asociaciones de hosts de la lista después de activar la regla**.

7 Haga clic en **Siguiente**.

8 Revise la lista de reglas activas y haga clic en **Finalizar**.

Resultados

En la pestaña **Reglas de implementación**, la regla se muestra como activa en la columna Estado.

Pasos siguientes

- Vea las asociaciones de perfil de imagen, perfil de host y ubicación de un host. Consulte Ver asociaciones de hosts.
- Corrija los hosts que no cumplan con las reglas. Consulte Corregir un host no compatible.

Ver asociaciones de hosts

Algunos de los hosts de inventario de vSphere Auto Deploy probablemente no cumplan con las reglas de implementación activas. Para comprobar si uno o más hosts ESXi cumplen con el conjunto de reglas activas, debe comprobar el cumplimiento de las asociaciones de hosts.

Requisitos previos

- Prepare el sistema e instale el servidor Auto Deploy. Para obtener más información, consulte Preparar el sistema para vSphere Auto Deploy.
- Cree una regla de vSphere Auto Deploy. Consulte Crear una regla de implementación.
- Active una regla de vSphere Auto Deploy. Consulte Activar, desactivar y reordenar las reglas de implementación.

Procedimiento

1 En la página de inicio de vSphere Web Client, haga clic en **Auto Deploy**.

   De manera predeterminada, solo la función de administrador incluye privilegios para usar el servicio de vSphere Auto Deploy.

2 Comprobar el cumplimiento de las asociaciones de hosts

La ventana **Comprobar cumplimiento de asociaciones de hosts** muestra el estado actual del host y si este cumple con el conjunto de reglas activas. Puede ver el perfil de imagen, el perfil de host, la ubicación de host, el paquete de scripts y las asociaciones que están asignados actualmente y que entrarán en efecto después de corregir el host. Puede asignar un paquete de scripts a un host solo mediante el uso de cmdlets de PowerCLI.

Opción	Pasos
Si quiere comprobar el cumplimiento de las asociaciones de hosts de un solo host	1 En la pestaña **Hosts implementados**, seleccione un host ESXi. 2 Haga clic en **Comprobar cumplimiento de asociaciones de hosts**. 3 Compruebe si las asociaciones de hosts cumplen con el conjunto de reglas activas actual. 4 Cierre la ventana **Comprobar cumplimiento de asociaciones de hosts**. ■ Si quiere corregir el host, haga clic en **Corregir**. ■ Si no quiere corregir el host, haga clic en **Cerrar**.
Si quiere comprobar el cumplimiento de las asociaciones de hosts de varios hosts	1 En la pestaña **Hosts implementados**, use Mayús+clic izquierdo o Ctrl+clic izquierdo para seleccionar varios hosts ESXi. 2 Haga clic en **Comprobar cumplimiento de asociaciones de hosts**. 3 Confirme que quiere comprobar el cumplimiento de todos los hosts seleccionados. 4 Revise el estado de cumplimiento de los hosts en el panel izquierdo. 5 (Opcional) En el panel izquierdo, seleccione un host para ver detalles de estado de cumplimiento en el panel derecho. 6 (Opcional) Seleccione uno o varios hosts, y haga clic en **Corregir los hosts seleccionados** para corregirlos. ■ Haga clic en la casilla de verificación de cada host que quiera seleccionar. ■ Haga clic en la casilla de verificación **Hosts** para seleccionar todos los hosts. 7 Haga clic en **Cerrar** para cerrar la ventana **Comprobar cumplimiento de asociaciones de hosts**.

Pasos siguientes

- Corrija los hosts que no cumplan con las reglas. Consulte Corregir un host no compatible.
- Edite la asociación de perfil de imagen de un host. Consulte Editar la asociación de perfil de imagen de un host.
- Edite una regla de vSphere Auto Deploy. Consulte Editar una regla de implementación.

Editar la asociación de perfil de imagen de un host

Puede editar la asociación de perfil de imagen de un único host si el host no está asociado a ninguna regla de vSphere Auto Deploy o si no desea cambiar la asociación de perfil de imagen de varios hosts mediante la edición de una regla.

Requisitos previos

- Prepare el sistema e instale el servidor Auto Deploy. Para obtener más información, consulte Preparar el sistema para vSphere Auto Deploy.
- Cree una regla de vSphere Auto Deploy. Consulte Crear una regla de implementación.

- Active una regla de vSphere Auto Deploy. Consulte Activar, desactivar y reordenar las reglas de implementación.

Procedimiento

1 En la página de inicio de vSphere Web Client, haga clic en **Auto Deploy**.

De manera predeterminada, solo la función de administrador incluye privilegios para usar el servicio de vSphere Auto Deploy.

2 En la pestaña **Hosts implementados**, seleccione un host ESXi.

3 Haga clic en **Editar asociación de perfil de imagen**.

Aparece el cuadro de diálogo Editar asociación de perfil de imagen.

4 Edite la asociación de perfil de imagen del host.

Opción	Acción
Si no desea cambiar el perfil de imagen	Seleccione la opción **Mismo perfil de imagen**.
Si desea asignar un nuevo perfil de imagen a los hosts seleccionados	1 Seleccione la opción **Buscar perfil de imagen**. 2 Seleccione un almacén de software en el menú desplegable. 3 Seleccione un perfil de imagen de la lista. 4 (Opcional) Si desea omitir la verificación de nivel de aceptación para el perfil de imagen, active la casilla **Omitir comprobación de firma de perfil de imagen**.

5 Haga clic en **Aceptar**.

Resultados

El nuevo perfil de imagen aparece en la columna Perfil de imagen después de actualizar la página.

Pasos siguientes

- Vea las asociaciones de perfil de imagen, perfil de host y ubicación de un host. Consulte Ver asociaciones de hosts.
- Si el host está asociado a una regla y desea revertirlo al perfil de imagen definido en la regla, debe corregir el host. Consulte Corregir un host no compatible.

Corregir un host no compatible

Cuando se agrega una regla al conjunto de reglas activas de vSphere Auto Deploy o cuando se realizan cambios en una regla o más, los hosts no se actualizan automáticamente. Debe corregir las asociaciones de host para aplicar las nuevas reglas al host.

Requisitos previos

- Prepare el sistema e instale el servidor Auto Deploy. Para obtener más información, consulte Preparar el sistema para vSphere Auto Deploy.

- Cree una regla de vSphere Auto Deploy. Consulte Crear una regla de implementación.
- Active una regla de vSphere Auto Deploy. Consulte Activar, desactivar y reordenar las reglas de implementación.
- Si al corregir un host se produce un cambio en su ubicación, debe ponerse al host en modo de mantenimiento.

Procedimiento

1 En la página de inicio de vSphere Web Client, haga clic en **Auto Deploy**.

   De manera predeterminada, solo la función de administrador incluye privilegios para usar el servicio de vSphere Auto Deploy.

2 En la pestaña **Hosts implementados**, seleccione un host ESXi.

   Puede usar Mayús+clic izquierdo o Ctrl+clic izquierdo para seleccionar varios hosts.

3 Haga clic en **Corregir asociaciones de hosts**.

   Si corrige un host que tiene una asociación de perfil de imagen editada, el host vuelve a la configuración definida en la regla con la que coincide.

   Puede supervisar el progreso del proceso de corrección en el panel Tareas recientes.

Pasos siguientes

- Vea las asociaciones de perfil de imagen, perfil de host y ubicación de un host. Consulte Ver asociaciones de hosts.
- Cambie la asociación de perfil de imagen de un host. Consulte Editar la asociación de perfil de imagen de un host.

Agregar un host al inventario de vSphere Auto Deploy

Puede ver los hosts que no coinciden con ninguna de las reglas de vSphere Auto Deploy y agregar manualmente un host al inventario de vSphere Auto Deploy.

Para agregar un host al inventario actual de hosts implementados de vSphere Auto Deploy, puede crear una nueva regla o editar una regla existente para incluir un host no implementado con vSphere Auto Deploy y asociarlo con un perfil de imagen, perfil de host y ubicación específicos. Como alternativa, puede agregar un host manualmente al inventario asignándole un perfil de imagen, un perfil de host y una ubicación.

Requisitos previos

- Prepare el sistema e instale el servidor Auto Deploy. Para obtener más información, consulte Preparar el sistema para vSphere Auto Deploy.

- Para asignar un perfil de imagen al host, agregue al inventario el almacén de software que necesita. Consulte Agregar un almacén de software o Importar un almacén de software.

Procedimiento

1 Iniciar el asistente Agregar al inventario

  Puede agregar un host que no corresponda a ninguna regla de vSphere Auto Deploy a la lista de hosts implementados mediante el uso del asistente Agregar al inventario.

2 Seleccionar un perfil de imagen en el asistente Agregar al inventario

  Usted tiene la opción de asignar un perfil de imagen a un host que quiera agregar al inventario de vSphere Auto Deploy.

3 Seleccionar un perfil de host en el asistente Agregar al inventario

  Puede elegir asignar un perfil de host a un host que quiera agregar al inventario de vSphere Auto Deploy.

4 Seleccionar una ubicación de host en el asistente Agregar al inventario

  Puede asignar una ubicación a un host que quiera agregar al inventario de vSphere Auto Deploy.

5 Ver el resumen del asistente Agregar al inventario

  Puede revisar las asociaciones de hosts antes de completar el asistente Agregar al inventario.

Pasos siguientes

- Edite una regla de vSphere Auto Deploy. Consulte Editar una regla de implementación.
- Vea las asociaciones de perfil de imagen, perfil de host y ubicación de un host. Consulte Ver asociaciones de hosts.
- Corrija los hosts que no cumplan con las reglas. Consulte Corregir un host no compatible.

Iniciar el asistente Agregar al inventario

Puede agregar un host que no corresponda a ninguna regla de vSphere Auto Deploy a la lista de hosts implementados mediante el uso del asistente Agregar al inventario.

Procedimiento

1 En la página de inicio de vSphere Web Client, haga clic en **Auto Deploy**.

  De manera predeterminada, solo la función de administrador incluye privilegios para usar el servicio de vSphere Auto Deploy.

2 En la pestaña **Hosts detectados**, seleccione uno o más hosts que quiera aprovisionar con un perfil de imagen, un perfil de host y una ubicación.

3 Seleccione **Agregar al inventario**.

  Aparece el asistente Agregar al inventario.

Seleccionar un perfil de imagen en el asistente Agregar al inventario

Usted tiene la opción de asignar un perfil de imagen a un host que quiera agregar al inventario de vSphere Auto Deploy.

Requisitos previos

Para asignar un perfil de imagen al host, agregue al inventario el almacén de software que necesita. Consulte Agregar un almacén de software o Importar un almacén de software.

Procedimiento

1 Seleccione un almacén de software en el menú desplegable.

2 Seleccione un perfil de imagen en la lista de perfiles de imágenes en el almacén seleccionada.

3 Si desea omitir la verificación de nivel de aceptación del perfil de imagen, active la casilla **Omitir comprobación de firma de perfil de imagen**.

4 Seleccione un perfil de imagen.

5 Haga clic en **Siguiente**.

Seleccionar un perfil de host en el asistente Agregar al inventario

Puede elegir asignar un perfil de host a un host que quiera agregar al inventario de vSphere Auto Deploy.

Procedimiento

1 En la página Seleccionar perfil de host del asistente, seleccione un perfil de host.

Opción	Acción
Si no desea asignar un perfil de host a los hosts seleccionados	Active la casilla **No incluir un perfil de host**.
Si desea asignar un perfil de host a los hosts seleccionados	Seleccione un perfil de host de la lista.

2 Haga clic en **Siguiente**.

Seleccionar una ubicación de host en el asistente Agregar al inventario

Puede asignar una ubicación a un host que quiera agregar al inventario de vSphere Auto Deploy.

Procedimiento

1 Seleccione un centro de datos, una carpeta o un clúster como ubicación del host.

2 Haga clic en **Siguiente**.

Ver el resumen del asistente Agregar al inventario

Puede revisar las asociaciones de hosts antes de completar el asistente Agregar al inventario.

Procedimiento

1 En la página Listo para finalizar, revise las asociaciones de hosts seleccionadas.

2 Haga clic en **Finalizar**.

Aprovisionar sistemas ESXi con vSphere Auto Deploy

vSphere Auto Deploy puede aprovisionar cientos de hosts físicos con el software ESXi. Se pueden aprovisionar los hosts que no ejecutaron previamente el software ESXi (primer arranque), así como reiniciar o reaprovisionar los hosts con un perfil de imagen, un perfil de host, un script personalizado o una ubicación de clúster o carpeta diferentes.

El proceso de vSphere Auto Deploy varía según el estado del host y según los cambios que desea realizar el usuario.

Aprovisionar un host (primer arranque)

Aprovisionar un host que nunca se aprovisionó con vSphere Auto Deploy (primer arranque) es una acción diferente a los procesos de arranque subsiguientes. Es necesario preparar el host y cumplir con todos los otros requisitos previos para poder aprovisionar el host. También puede definir un perfil de imagen personalizado con vSphere ESXi Image Builder mediante los cmdlets de vSphere Web Client o PowerCLI.

Requisitos previos

- Asegúrese de que el host cumpla con los requisitos de hardware para los hosts ESXi.

  Consulte Requisitos de hardware de ESXi.
- Prepare el sistema para vSphere Auto Deploy. Consulte Prepararse para vSphere Auto Deploy.
- Escriba reglas para asignar un perfil de imagen al host y para asignar, de forma opcional, un perfil de host y una ubicación de vCenter Server al host. Consulte Administrar vSphere Auto Deploy con cmdlets de PowerCLI o Administrar vSphere Auto Deploy con vSphere Web Client.

  Cuando se complete la instalación, el servicio vSphere Auto Deploy estará habilitado, la configuración de DHCP estará completada y las reglas para el host que desea aprovisionar se encontrarán en el conjunto de reglas activas.

Procedimiento

1 Encienda el host.

  El host se comunica con el servidor DHCP y descarga iPXE desde la ubicación que el servidor indica. A continuación, el servidor vSphere Auto Deploy aprovisiona al host con la imagen especificada por el motor de reglas. El servidor vSphere Auto Deploy también puede aplicar un perfil de host al host si existe uno especificado en el conjunto de reglas. Por último, vSphere Auto Deploy agrega el host al sistema vCenter Server especificado en el conjunto de reglas.

2 (opcional) Si vSphere Auto Deploy aplica un perfil de host que requiere alguna entrada del usuario, como una dirección IP, el host se coloca en el modo de mantenimiento. Vuelva a aplicar el perfil de host con vSphere Web Client y proporcione las entradas del usuario cuando se solicite.

Resultados

Después de un proceso de primer arranque, el host se ejecuta y administra a través de un sistema vCenter Server. vCenter Server almacena la información del perfil de imagen, el perfil de host y la ubicación del host.

Ahora puede reiniciar el host según sea necesario. Cada vez que reinicie, el host se reaprovisionará a través del sistema vCenter Server.

Pasos siguientes

Reaprovisione los hosts según sea necesario. Consulte Reaprovisionar hosts.

Si quiere cambiar el perfil de imagen, el perfil de host, el script personalizado o la ubicación del host, actualice las reglas y actívelas mediante vSphere Web Client o realice una operación de cumplimiento de prueba y reparación en una sesión de PowerCLI. Consulte Reglas y conjuntos de reglas o Probar y reparar cumplimiento de reglas .

Reaprovisionar hosts

vSphere Auto Deploy admite varias opciones de reaprovisionamiento. Puede realizar un reinicio o un reaprovisionamiento sencillos con otro perfil de imagen o de host.

Para un primer arranque con vSphere Auto Deploy, debe configurar el entorno y agregar reglas al conjunto de reglas. Consulte Prepararse para vSphere Auto Deploy.

Están disponibles las siguientes operaciones de reaprovisionamiento.

- Reinicio simple.
- Reinicio de hosts sobre los que el usuario respondió preguntas durante la operación de arranque.
- Reaprovisionamiento con un perfil de imagen diferente.
- Reaprovisionamiento con un perfil de host diferente.

Reaprovisionar hosts con operaciones de reinicio simples

El reinicio simple de un host aprovisionado con vSphere Auto Deploy solo requiere que se sigan cumpliendo todos los requisitos previos. El proceso utiliza el perfil de imagen asignado previamente, el perfil de host, el script personalizado y la ubicación de vCenter Server.

Requisitos previos

- Compruebe que la configuración que realizó durante la primera operación de arranque esté vigente. Consulte Aprovisionar un host (primer arranque).
- Compruebe que todos los elementos asociados se encuentren disponibles. Un elemento puede ser un perfil de imagen, un perfil de host, un script personalizado o una ubicación de inventario de vCenter Server.
- Compruebe que el host contenga la información de identificación (etiqueta de activo, dirección IP) que tenía en las operaciones de arranque anteriores.

Procedimiento

1 Coloque el host en modo de mantenimiento.

Tipo de host	Acción
El host es parte de un clúster de DRS	VMware DRS migra las máquinas virtuales a los hosts adecuados cuando coloca el host en modo de mantenimiento.
El host no es parte de un clúster de DRS	Debe migrar todas las máquinas virtuales a distintos hosts y poner todos los hosts en modo de mantenimiento.

2 Reinicie el host.

Resultados

El host se apaga. Al reiniciarse, el host utiliza el perfil de imagen que proporciona el servidor vSphere Auto Deploy. El servidor vSphere Auto Deploy también aplica el perfil de host almacenado en el sistema vCenter Server.

Reaprovisionar un host con un nuevo perfil de imagen mediante PowerCLI

Es posible usar vSphere Auto Deploy para reaprovisionar un host con un perfil de imagen nuevo en una sesión de PowerCLI si se cambia la regla para el host y se ejecuta una operación de prueba y reparación de cumplimiento.

Existen varias opciones para reaprovisionar hosts.

- Si los VIB que desea usar son compatibles con la actualización directa, puede usar un comando `esxcli software vib`. En ese caso, también debe actualizar el conjunto de reglas que se va a usar en un perfil de imagen que incluya los nuevos VIB.
- Durante las pruebas, puede aplicar un perfil de imagen a un host individual con el cmdlet `Apply-EsxImageProfile` y reiniciar el host para que el cambio sea efectivo. El cmdlet `Apply-EsxImageProfile` actualiza la asociación entre el host y el perfil de imagen, pero no instala ningún VIB en el host.
- En todos los demás casos, utilice este procedimiento.

Requisitos previos

- Compruebe que el perfil de imagen que desea utilizar para reaprovisionar el host se encuentre disponible. Utilice vSphere ESXi Image Builder en una sesión de PowerCLI. Consulte Personalizar instalaciones con vSphere ESXi Image Builder.
- Compruebe que la configuración que realizó durante la primera operación de arranque esté vigente.

Procedimiento

1 En la indicación de PowerShell, ejecute el cmdlet `Connect-VIServer` PowerCLI para conectarse al sistema vCenter Server con el que se registró vSphere Auto Deploy.

```
Connect-VIServer ipv4_or_ipv6_address
```

Es posible que el cmdlet devuelva una advertencia de certificado de servidor. En un entorno de producción, asegúrese de que no se emita ninguna advertencia de certificado de servidor. En un entorno de desarrollo, puede omitir la advertencia.

2 Determine la ubicación de un almacén de software público que contenga el perfil de imagen que desea utilizar o defina un perfil de imagen personalizado con vSphere ESXi Image Builder.

3 Ejecute `Add-EsxSoftwareDepot` para agregar el almacén de software que contiene el perfil de imagen a la sesión de PowerCLI.

Tipo de almacén	Cmdlet
Almacén remoto	Ejecute **`Add-EsxSoftwareDepot`** ***`depot_url`***.
Archivo ZIP	a Descargue el archivo ZIP en una ruta de acceso de archivos local o cree un punto de montaje local en el equipo de PowerCLI. b Ejecute **`Add-EsxSoftwareDepot C:\`*****`file_path`*****`\`*****`my_offline_depot`*****`.zip`**.

4 Ejecute `Get-EsxImageProfile` para ver una lista de perfiles de imagen y determine qué perfil desea utilizar.

5 Ejecute `Copy-DeployRule` y especifique el parámetro `ReplaceItem` para cambiar la regla que asigna un perfil de imagen a hosts.

El siguiente cmdlet reemplaza el perfil de imagen actual que la regla asigna al host con el perfil *my_new_imageprofile*. Cuando el cmdlet finaliza, `myrule` asigna el nuevo perfil de imagen a los hosts. Se cambia el nombre de la antigua versión de `myrule` y se la oculta.

```
Copy-DeployRule myrule -ReplaceItem my_new_imageprofile
```

6 Pruebe el cumplimiento de reglas para cada host en el que desee implementar la imagen.

a Compruebe que pueda acceder al host para el cual desea probar el cumplimiento del conjunto de reglas.

```
Get-VMHost -Name ESXi_hostname
```

b Ejecute el cmdlet que prueba el cumplimiento del conjunto de reglas para el host y vincule el valor devuelto a una variable para usarlo en otro momento.

```
$tr = Test-DeployRuleSetCompliance ESXi_hostname
```

c Examine las diferencias entre el contenido del conjunto de reglas y la configuración del host.

```
$tr.itemlist
```

El sistema devolverá una tabla de elementos actuales y esperados si el host en el que se desea probar el cumplimiento de un nuevo conjunto de reglas cumple con el conjunto de reglas activo.

```

CurrentItem                          ExpectedItem
-----------                          ------------
my_old_imageprofilemy_new_imageprofile
```

d Corrija el host para que use el conjunto de reglas modificado la próxima vez que arranque.

```
Repair-DeployRuleSetCompliance $tr
```

7 Reinicie el host para aprovisionarlo con el nuevo perfil de imagen.

Reaprovisionar un host con un nuevo perfil de imagen mediante vSphere Web Client

Puede usar vSphere Auto Deploy para reaprovisionar un host con un nuevo perfil de imagen con vSphere Web Client cambiando la regla a la que corresponde el host y activándola.

Requisitos previos

- Compruebe que el perfil de imagen que desea utilizar para reaprovisionar el host se encuentre disponible. Consulte Crear un perfil de imagen.
- Compruebe que la configuración que realizó durante la primera operación de arranque esté vigente.

Procedimiento

1 En la página de inicio de vSphere Web Client, haga clic en **Auto Deploy**.

De manera predeterminada, solo la función de administrador incluye privilegios para usar el servicio de vSphere Auto Deploy.

2 En la pestaña **Reglas de implementación**, seleccione la regla que desea editar en la lista de reglas del inventario y haga clic en **Editar**.

Se mostrará el cuadro de diálogo Editar regla de implementación.

3 Seleccione la página **Seleccionar perfil de imagen** para asignar un perfil de imagen a los hosts que coincidan con los criterios de la regla.

Opción	Acción
Si no desea cambiar el perfil de imagen	Seleccione la opción **Mismo perfil de imagen**.
Si no desea asignar un perfil de imagen a los hosts seleccionados	Seleccione la opción **Sin perfil de imagen**.
Si desea asignar un nuevo perfil de imagen a los hosts seleccionados	1 Seleccione la opción **Buscar perfil de imagen**. 2 Seleccione un almacén de software en el menú desplegable. 3 Seleccione un perfil de imagen de la lista. 4 (Opcional) Si desea omitir la verificación de nivel de aceptación para el perfil de imagen, active la casilla **Omitir comprobación de firma de perfil de imagen**.

4 Haga clic en **Activar/desactivar reglas**.

5 En la lista de reglas inactivas, seleccione la regla que desea activar y haga clic en el botón **Activar**.

6 (opcional) Si desea reordenar las reglas de la lista de reglas activas, seleccione la regla que desea mover hacia arriba o hacia abajo en la lista, y haga clic en los iconos **Subir** o **Bajar** sobre la lista de reglas activas.

   Las reglas se ordenan por prioridad. Por ejemplo, si se aplican dos o más reglas al mismo host, pero se definen de manera que aprovisionarán el host con perfiles de imagen, perfiles de host y ubicaciones diferentes, la regla con la posición más alta de la lista se aplica al host.

7 (opcional) Si desea probar una regla inactiva antes de activarla, active la casilla **Probar reglas antes de activación** y haga clic en **Siguiente**.

   a En la página Seleccionar destinos de prueba del asistente, en la pestaña **Filtrar**, seleccione los hosts en los que desea probar la regla inactiva y haga clic en **Siguiente**.

      En la pestaña **Seleccionado**, solo se muestran los hosts seleccionados.

   b En la página Vista previa de resultados de la prueba del asistente, seleccione un host de la lista para ver el estado actual del host y los cambios que se esperan después de la activación de la regla.

      Si el host cumple con la regla, no es necesario corregir el host tras activar la regla.

   c (opcional) Si desea corregir los hosts seleccionados después de la activación de la regla, active la casilla **Corregir asociaciones de hosts de la lista después de activar la regla**.

8 Haga clic en **Siguiente**.

9 Revise la lista de reglas activas y haga clic en **Finalizar**.

10 Reinicie el host para aprovisionarlo con el nuevo perfil de imagen.

Actualizar la personalización de hosts en vSphere Web Client

Si un host requería la intervención del usuario durante un arranque anterior, las respuestas estarán guardadas con vCenter Server. Si desea solicitar información nueva al usuario, debe corregir el host.

Requisitos previos

Conecte un perfil de host que solicite entrada de datos del usuario en el host.

Procedimiento

1 Migre todas las máquinas virtuales a distintos hosts y ponga el host en modo de mantenimiento.

Tipo de host	Acción
El host es parte de un clúster de DRS	VMware DRS migra las máquinas virtuales a los hosts adecuados cuando coloca el host en modo de mantenimiento.
El host no es parte de un clúster de DRS	Debe migrar todas las máquinas virtuales a distintos hosts y poner todos los hosts en modo de mantenimiento.

2 En la página de inicio de vSphere Web Client, haga clic en **Auto Deploy**.

De manera predeterminada, solo la función de administrador incluye privilegios para usar el servicio de vSphere Auto Deploy.

3 En la pestaña **Hosts implementados**, seleccione un host ESXi.

4 Haga clic en **Corregir asociaciones de hosts**.

Puede supervisar el progreso del proceso de corrección en el panel Tareas recientes.

5 Cuando se le solicite, proporcione la entrada de datos del usuario.

6 Dirija el host para salir del modo de mantenimiento.

Resultados

La personalización del host se guarda y se aplicará la próxima vez que arranque el host.

Usar vSphere Auto Deploy para almacenamiento en caché sin estado e instalaciones con estado

La función de almacenamiento en caché sin estado de vSphere Auto Deploy permite almacenar la imagen del host en la memoria caché. La función de instalaciones con estado de vSphere Auto Deploy permite instalar hosts por medio de la red. Después del primer arranque de red, estos hosts arrancan como cualquier otro host ESXi.

La solución de almacenamiento en caché sin estado está destinada principalmente a las situaciones en las que varios hosts arrancan en simultáneo. La imagen almacenada en la memoria caché local ayuda a prevenir un cuello de botella que se produce si cientos de hosts se conectan simultáneamente al servidor vSphere Auto Deploy. Una vez finalizada la operación de arranque, los hosts se conectan a vSphere Auto Deploy para completar la configuración.

La característica de instalaciones con estado permite aprovisionar hosts con el perfil de imagen por medio de la red sin necesidad de configurar la infraestructura de arranque PXE.

- Introducción a almacenamiento en caché sin estado e instalaciones con estado

  Es posible usar el perfil de host de Configuración de la memoria caché del sistema para aprovisionar hosts con almacenamiento en caché sin estado e instalaciones con estado de vSphere Auto Deploy.

- Descripción general de las instalaciones con estado y el almacenamiento en caché sin estado

  Cuando desee utilizar vSphere Auto Deploy con almacenamiento en caché sin estado o con instalaciones con estado, deberá configurar un perfil de host, aplicar dicho perfil y establecer el orden de arranque.

- Configurar un perfil de host para utilizar el almacenamiento en caché sin estado

  Si se configura un host para utilizar el almacenamiento en caché sin estado, el host utiliza una imagen en la memoria caché cuando el servidor vSphere Auto Deploy no está disponible. Para utilizar el almacenamiento en caché sin estado, debe configurar un perfil de host. Puede aplicar ese perfil a otros hosts que desee configurar para el almacenamiento en caché sin estado.

- Configurar un perfil de host para habilitar instalaciones con estado

  Si desea configurar un host aprovisionado con vSphere Auto Deploy para el arranque desde el disco, debe configurar un perfil de host. Es posible aplicar ese perfil de host a otros hosts que desee configurar para instalaciones con estado.

Introducción a almacenamiento en caché sin estado e instalaciones con estado

Es posible usar el perfil de host de Configuración de la memoria caché del sistema para aprovisionar hosts con almacenamiento en caché sin estado e instalaciones con estado de vSphere Auto Deploy.

Ejemplos de almacenamiento en caché sin estado e instalaciones con estado

Hosts aprovisionados con vSphere Auto Deploy que almacenan en caché la imagen (almacenamiento en caché sin estado)

Configure y aplique un perfil de host para el almacenamiento en caché sin estado. Puede almacenar la imagen en la memoria caché de un disco local, un disco remoto o una unidad USB. Continúe aprovisionando este host con vSphere Auto Deploy. Si el servidor vSphere Auto Deploy no está disponible, por ejemplo, debido a que cientos de hosts intentan acceder a él de forma simultánea, el host arranca desde la memoria caché. Después de la operación de arranque, el host intenta comunicarse con el servidor vSphere Auto Deploy para completar la configuración.

Los hosts aprovisionados con vSphere Auto Deploy se convierten en hosts con estado

Configure y aplique un perfil de host para instalaciones con estado. Cuando aprovisiona un host con vSphere Auto Deploy, la imagen se instala en el disco local, un disco remoto o una

unidad USB. Para arranques posteriores, hágalo desde el disco. El host ya no usa vSphere Auto Deploy.

Preparar

Para usar correctamente el almacenamiento en caché sin estado o instalaciones con estado, debe decidir cómo configurar el sistema y establecer el orden de arranque.

Tabla 2-17. Preparar almacenamiento en caché sin estado o instalaciones con estado

Requisito o decisión	Descripción
Decidir sobre la sobrescritura de la partición de VMFS	Cuando instale ESXi mediante el instalador interactivo, se le consulta si desea sobrescribir un almacén de datos existente de VMFS. El perfil de host de Configuración de la memoria caché del sistema proporciona una opción para sobrescribir particiones existentes de VMFS. La opción no está disponible si configura el perfil de host para que use una unidad USB.
Decidir si se necesita un entorno de alta disponibilidad	Si usa vSphere Auto Deploy con almacenamiento en caché sin estado, puede configurar un entorno de vSphere Auto Deploy de alta disponibilidad para garantizar que las máquinas virtuales migren a hosts aprovisionados recientemente y que el entorno admita vNetwork Distributed Switch incluso si el sistema vCenter Server queda temporalmente no disponible.
Establecer el orden de arranque	El orden de arranque que especifica para los hosts depende de la característica que desea usar. ■ Para configurar vSphere Auto Deploy con almacenamiento en caché sin estado, configure el host para que primero intente arrancar desde la red y, luego, intente arrancar desde el disco. Si el servidor vSphere Auto Deploy no está disponible, el host arranca usando la memoria caché. ■ Para configurar vSphere Auto Deploy para instalaciones con estado en hosts que actualmente no tienen un disco de arranque, configure sus hosts para que primero intenten arrancar desde el disco y, luego, intenten hacerlo desde la red. **Nota** Si actualmente tiene una imagen de arranque en el disco, configure los hosts para un arranque PXE único y aprovisione el host con vSphere Auto Deploy para que use un perfil de host que especifique instalaciones con estado.

Almacenamiento en caché sin estado y pérdida de conectividad

Si los hosts ESXi que se ejecutan en las máquinas virtuales pierden conectividad con el servidor vSphere Auto Deploy, el sistema vCenter Server, o ambos, se aplicarán algunas limitaciones la próxima vez que reinicie el host.

- Si vCenter Server está disponible, pero el servidor vSphere Auto Deploy no lo está, los hosts no se conectan al sistema vCenter Server de forma automática. Puede conectar manualmente los hosts a vCenter Server o esperar hasta que el servidor vSphere Auto Deploy vuelva a estar disponible.
- Si tanto vCenter Server como vSphere Auto Deploy no están disponibles, puede conectarse a cada host ESXi mediante VMware Host Client y agregar máquinas virtuales a cada host.
- Si vCenter Server no está disponible, vSphere DRS no funciona. El servidor vSphere Auto Deploy no puede agregar hosts a vCenter Server. Puede conectarse a cada host ESXi mediante VMware Host Client y agregar máquinas virtuales a cada host.
- Si realiza cambios a la configuración mientras está perdida la conectividad, los cambios se pierden cuando se restaura la conexión del servidor vSphere Auto Deploy.

Descripción general de las instalaciones con estado y el almacenamiento en caché sin estado

Cuando desee utilizar vSphere Auto Deploy con almacenamiento en caché sin estado o con instalaciones con estado, deberá configurar un perfil de host, aplicar dicho perfil y establecer el orden de arranque.

Cuando se aplica un perfil de host que permite el almacenamiento en caché en un host, vSphere Auto Deploy particiona el disco especificado. Lo que ocurre después depende de la forma en que configure el perfil de host y establezca el orden de arranque en el host.

- Si se ha seleccionado **Habilitar almacenamiento en caché sin estado en el host** en el perfil de host de configuración de caché del sistema, vSphere Auto Deploy almacenará la imagen en caché cuando aplique el perfil de host. No se requiere reiniciar. Cuando reinicie más tarde, el host continuará utilizando la infraestructura de vSphere Auto Deploy para recuperar su imagen. Si el servidor vSphere Auto Deploy no está disponible, el host utiliza la imagen almacenada en caché.
- vSphere Auto Deploy instala la imagen si **Habilitar instalaciones con estado en el host** está seleccionado en el perfil de host de configuración de caché del sistema. Al reiniciar, el host inicialmente arranca usando vSphere Auto Deploy para completar la instalación. A continuación se genera automáticamente un reinicio, después del cual el host arranca desde el disco, al igual que un host aprovisionado con el instalador. vSphere Auto Deploy ya no realiza el aprovisionamiento del host.

Puede aplicar el perfil del host desde vSphere Web Client o escribir una regla de vSphere Auto Deploy en una sesión de PowerCLI que aplique el perfil del host.

Usar vSphere Web Client para configurar vSphere Auto Deploy para el almacenamiento en caché sin estado o las instalaciones con estado

Puede crear un perfil de host en un host de referencia y aplicar dicho perfil de host a hosts adicionales, o a una carpeta o clúster de vCenter Server. Aparece el siguiente flujo de trabajo.

1 Aprovisione un host con vSphere Auto Deploy y edite el perfil de host de configuración de caché de imagen del sistema del host.

2 Coloque uno más hosts de destino en el modo de mantenimiento, aplique el perfil de host a cada host e indique al host que salga del modo de mantenimiento.

3 Lo que ocurra después depende del perfil de host seleccionado.

   - Si el perfil de host habilitó el almacenamiento en caché sin estado, la imagen se almacenará en caché en el disco. No se requiere reiniciar.
   - Si el perfil de host habilitó las instalaciones con estado, se instalará la imagen. Cuando reinicie, el host utilizará la imagen instalada.

Usar PowerCLI para configurar vSphere Auto Deploy para el almacenamiento en caché sin estado o las instalaciones con estado

Puede crear un perfil de host para un host de referencia y escribir una regla de vSphere Auto Deploy que aplique dicho perfil de host a otros hosts de destino en una sesión de PowerCLI. Aparece el siguiente flujo de trabajo.

1 Aprovisione un host de referencia con vSphere Auto Deploy y cree un perfil de host para habilitar una forma de almacenamiento en caché.

2 Escriba una regla que aprovisione hosts adicionales con vSphere Auto Deploy y que aplique el perfil de host de referencia a esos hosts.

3 vSphere Auto Deploy aprovisiona cada host con el perfil de imagen o mediante el uso del paquete de scripts asociado con la regla. El efecto exacto de aplicar el perfil de host depende del perfil del host seleccionado.

   - En el caso de instalaciones con estado, vSphere Auto Deploy procederá de la siguiente manera:
     - Durante el primer arranque, vSphere Auto Deploy instala la imagen en el host.
     - Durante los arranques siguientes, el host arranca desde el disco. Los hosts no necesitan una conexión al servidor vSphere Auto Deploy.
   - En el caso del almacenamiento en caché sin estado, vSphere Auto Deploy procederá de la siguiente manera:
     - Durante el primer arranque, vSphere Auto Deploy aprovisiona el host y almacena la imagen en caché.
     - Durante los arranques siguientes, vSphere Auto Deploy aprovisiona el host. Si vSphere Auto Deploy no está disponible, el host arranca desde la imagen almacenada en caché. Sin embargo, la configuración solo puede completarse cuando el host puede llegar al servidor vSphere Auto Deploy.

Configurar un perfil de host para utilizar el almacenamiento en caché sin estado

Si se configura un host para utilizar el almacenamiento en caché sin estado, el host utiliza una imagen en la memoria caché cuando el servidor vSphere Auto Deploy no está disponible. Para utilizar el almacenamiento en caché sin estado, debe configurar un perfil de host. Puede aplicar ese perfil a otros hosts que desee configurar para el almacenamiento en caché sin estado.

Requisitos previos

- Decida qué disco desea utilizar para almacenamiento en caché y determine si el proceso de almacenamiento en caché sobrescribirá una partición de VMFS existente.
- En los entornos de producción, incluya el sistema vCenter Server y el servidor vSphere Auto Deploy en un entorno altamente disponible para protegerlos. Tener vCenter Server en un clúster de administración garantiza que VDS y la migración de máquinas virtuales estén disponibles. De ser posible, proteja también otros elementos de la infraestructura. Consulte Set Up Highly Available vSphere Auto Deploy Infrastructure.
- Configure el entorno de vSphere Auto Deploy. Consulte Prepararse para vSphere Auto Deploy.
- Compruebe que haya un disco con al menos 1 GB de espacio libre disponible. Si el disco aún no está particionado, este procedimiento se lleva a cabo cuando aplica el perfil de host.
- Configure el host para que primero intente realizar un arranque de red y, si se produce un error, un arranque desde un disco. Consulte la documentación del proveedor de hardware.
- Cree un perfil de host. Consulte la documentación sobre *perfiles de host*.

Procedimiento

1. En la página de inicio de vSphere Web Client, haga clic en **Perfiles de host**.
2. Seleccione el perfil de host que desea configurar y elija la pestaña **Administrar**.
3. Haga clic en **Editar perfil de host**.
4. Conserve el nombre y la descripción, y haga clic en **Siguiente**.
5. En la página Editar perfil de host del asistente, seleccione **Opciones de configuración avanzadas > Configuración de memoria caché de imagen del sistema > Configuración de memoria caché de imagen del sistema**.
6. En el menú desplegable **Configuración de perfil de memoria caché de imagen del sistema**, elija una opción de directiva.

Opción	Descripción
Habilitar almacenamiento en caché sin estado en el host	Almacena en caché la imagen en el disco.
Habilitar almacenamiento en caché sin estado en un disco USB del host	Almacena en caché la imagen en un disco USB asociado al host.

7 (opcional) Si selecciona **Habilitar almacenamiento en caché sin estado en el host**, especifique la información sobre el disco que desea utilizar.

Opción	Descripción
Argumentos para el primer disco	De forma predeterminada, el sistema intenta reemplazar una instalación de ESXi existente y, a continuación, intenta escribir en el disco local. Puede utilizar el campo **Argumentos para primer disco** para especificar una lista separada por comas de los discos que se van a utilizar, en orden de preferencia. Puede especificar más de un disco. Utilice `esx` para el primer disco que tenga ESX instalado, use la información del modelo y del proveedor, o bien especifique el nombre del controlador de dispositivos vmkernel. Por ejemplo, para que el sistema busque primero un disco con el nombre de modelo ST3120814A, segundo cualquier disco que utilice el controlador mptsas y tercero el disco local, especifique `ST3120814A,mptsas,local` como el valor para el campo. La primera configuración de disco del perfil de host especifica el orden de búsqueda para determinar qué disco se va a usar para la memoria caché. El orden de búsqueda se especifica como una lista de valores delimitados por comas. El valor predeterminado `localesx,local` especifica que vSphere Auto Deploy primero debe buscar un disco de memoria caché local existente. El disco de memoria caché se identifica como un disco con la imagen del software ESXi existente. Si vSphere Auto Deploy no puede encontrar un disco de memoria caché existente, busca un dispositivo de disco local disponible. Al buscar un disco disponible, vSphere Auto Deploy usa el primer disco vacío que no contenga una partición de VMFS existente. Puede utilizar el primer argumento de disco solo para especificar el orden de búsqueda. No puede especificar un disco explícitamente. Por ejemplo, no puede especificar un determinado LUN o una SAN.
Marcar para sobrescribir los volúmenes VMFS en el disco seleccionado	Si activa esta casilla, el sistema sobrescribe los volúmenes VMFS existentes cuando no haya suficiente espacio disponible para almacenar la imagen, el perfil de imagen y el perfil de host.
Marcar para ignorar los dispositivos SSD conectados al host	Si activa esta casilla, el sistema omite todos los dispositivos SSD existentes y no almacena los perfiles de imagen ni los perfiles de host en ellos.

8 Haga clic en **Finalizar** para completar la configuración del perfil de host.

Pasos siguientes

Utilice la función de perfiles de host de vSphere Web Client para aplicar el perfil de host a hosts individuales. Consulte la documentación sobre *perfiles de host*. Como alternativa, puede crear una regla para asignar el perfil de host a los hosts con vSphere Web Client o PowerCLI. Consulte Escribir una regla y asignar un perfil de host a hosts.

- Cree una regla que aplique el perfil de host a todos los hosts que desea aprovisionar con la configuración especificada en el host de referencia. Para escribir una regla en una sesión de PowerCLI, consulte Escribir una regla y asignar un perfil de host a hosts.
- Si los hosts ya se aprovisionaron con vSphere Auto Deploy, ejecute la prueba y repare las operaciones de cumplimiento en una sesión de PowerCLI. Para eso, consulte Probar y reparar cumplimiento de reglas .

- Encienda los hosts no aprovisionados para aprovisionarlos con el nuevo perfil de host.

Configurar un perfil de host para habilitar instalaciones con estado

Si desea configurar un host aprovisionado con vSphere Auto Deploy para el arranque desde el disco, debe configurar un perfil de host. Es posible aplicar ese perfil de host a otros hosts que desee configurar para instalaciones con estado.

Puede configurar el perfil de host en un único host. También puede crear un perfil de host en un host de referencia y aplicarlo a otros hosts.

Requisitos previos

- Decida qué disco desea usar para almacenar la imagen y determine si la nueva imagen sobrescribirá una partición actual de VMFS.
- Configure el entorno de vSphere Auto Deploy. Consulte Prepararse para vSphere Auto Deploy.
- Compruebe que haya un disco con al menos 1 GB de espacio libre disponible. Si el disco aún no está particionado, este procedimiento se lleva a cabo cuando aplica el perfil de host.
- Configure el host para arrancar desde el disco. Consulte la documentación del proveedor de hardware.
- Cree un perfil de host. Consulte la documentación sobre *perfiles de host*.

Procedimiento

1. En la página de inicio de vSphere Web Client, haga clic en **Perfiles de host**.
2. Seleccione el perfil de host que desea configurar y elija la pestaña **Administrar**.
3. Haga clic en **Editar perfil de host**.
4. Conserve el nombre y la descripción, y haga clic en **Siguiente**.
5. En la página Editar perfil de host del asistente, seleccione **Opciones de configuración avanzadas > Configuración de memoria caché de imagen del sistema > Configuración de memoria caché de imagen del sistema**.
6. En el menú desplegable **Configuración de perfil de memoria caché de imagen del sistema**, elija una opción de directiva.

Opción	Descripción
Habilitar instalaciones con estado en el host	Almacena la imagen en la memoria caché, en un disco.
Habilitar instalaciones con estado en un disco USB del host	Almacena en caché la imagen en un disco USB asociado al host.

7 (opcional) Si selecciona la opción **Habilitar instalaciones con estado en el host**, especifique la información del disco que va a usar.

Opción	Descripción
Argumentos para el primer disco	De forma predeterminada, el sistema intenta reemplazar una instalación de ESXi existente y, a continuación, intenta escribir en el disco local. Puede utilizar el campo **Argumentos para primer disco** para especificar una lista separada por comas de los discos que se van a utilizar, en orden de preferencia. Puede especificar más de un disco. Utilice **`esx`** para el primer disco que tenga ESX instalado, use la información del modelo y del proveedor, o bien especifique el nombre del controlador de dispositivos vmkernel. Por ejemplo, para que el sistema busque primero un disco con el nombre de modelo ST3120814A, segundo cualquier disco que utilice el controlador mptsas y tercero el disco local, especifique **`ST3120814A,mptsas,local`** como el valor para el campo. La primera configuración de disco del perfil de host especifica el orden de búsqueda para determinar qué disco se va a usar para la memoria caché. El orden de búsqueda se especifica como una lista de valores delimitados por comas. El valor predeterminado **`localesx,local`** especifica que vSphere Auto Deploy primero debe buscar un disco de memoria caché local existente. El disco de memoria caché se identifica como un disco con la imagen del software ESXi existente. Si vSphere Auto Deploy no puede encontrar un disco de memoria caché existente, busca un dispositivo de disco local disponible. Al buscar un disco disponible, vSphere Auto Deploy usa el primer disco vacío que no contenga una partición de VMFS existente. Puede utilizar el primer argumento de disco solo para especificar el orden de búsqueda. No puede especificar un disco explícitamente. Por ejemplo, no puede especificar un determinado LUN o una SAN.
Marcar para sobrescribir los volúmenes VMFS en el disco seleccionado	Si activa esta casilla, el sistema sobrescribe los volúmenes VMFS existentes cuando no haya suficiente espacio disponible para almacenar la imagen, el perfil de imagen y el perfil de host.
Marcar para ignorar los dispositivos SSD conectados al host	Si activa esta casilla, el sistema omite todos los dispositivos SSD existentes y no almacena los perfiles de imagen ni los perfiles de host en ellos.

8 Haga clic en **Finalizar** para completar la configuración del perfil de host.

Pasos siguientes

Utilice la función de perfiles de host de vSphere Web Client para aplicar el perfil de host a hosts individuales. Consulte la documentación sobre *perfiles de host*. Como alternativa, puede crear una regla para asignar el perfil de host a los hosts con vSphere Web Client o PowerCLI. Consulte Escribir una regla y asignar un perfil de host a hosts.

- Cree una regla que aplique el perfil de host a todos los hosts que desea aprovisionar con la configuración especificada en el host de referencia. Para escribir una regla en una sesión de PowerCLI, consulte Escribir una regla y asignar un perfil de host a hosts.
- Si los hosts ya se aprovisionaron con vSphere Auto Deploy, ejecute la prueba y repare las operaciones de cumplimiento en una sesión de PowerCLI. Para eso, consulte Probar y reparar cumplimiento de reglas .

- Encienda los hosts no aprovisionados para aprovisionarlos con el nuevo perfil de host.

Configurar un host de referencia de vSphere Auto Deploy

En un entorno donde no se almacena ningún estado en el host, un host de referencia ayuda a configurar varios hosts con la misma configuración. Puede configurar el host de referencia con generación de registros, volcado de memoria y otra configuración que desea, guardar el perfil de host y escribir una regla que aplique el perfil de host a otros hosts según sea necesario.

Puede ajustar la configuración de almacenamiento, conexión de redes y seguridad en el host de referencia y configurar servicios, como syslog y NTP.

Información sobre la configuración del host de referencia

Un host de referencia bien diseñado se conecta con todos los servicios, como syslog, NTP, etc. La configuración del host de referencia también podría incluir seguridad, almacenamiento, conexión de redes y ESXi Dump Collector. Puede aplicar la configuración de dicho host a otros hosts a través de los perfiles de host.

La configuración exacta de su host de referencia depende de su entorno, pero podría considerar la siguiente personalización.

Configuración de servidor NTP

Al recopilar información de generación de registros en entornos grandes, deberá asegurarse que las horas de los registros se encuentren coordinadas. Configure el host de referencia para utilizar el servidor NTP en su entorno que todos los hosts puedan compartir. Puede especificar un servidor NTP ejecutando el comando `vicfg-ntp`. Puede iniciar y detener el servicio NTP para un host con el comando `vicfg-ntp` o con vSphere Web Client.

Configuración del servidor de syslog

Todos los hosts ESXi ejecutan un servicio de Syslog (`vmsyslogd`), que registra mensajes desde VMkernel y otros componentes del sistema en un archivo. Puede especificar el host de registro y administrar la ubicación, rotación, tamaño y otros archivos del registro ejecutando el comando de vCLI `esxcli system syslog` o a través de vSphere Web Client. La configuración de la generación de registros en un host remoto es especialmente importante para los hosts aprovisionados con vSphere Auto Deploy que no poseen almacenamiento local. Puede instalar opcionalmente vSphere Syslog Collector para recopilar registros de todos los hosts.

Configuración de volcados de memoria

Puede configurar su host de referencia para enviar volcados de memoria a un LUN SAN compartido o puede instalar ESXi Dump Collector en su entorno y configurar el host de referencia para utilizar ESXi Dump Collector. Consulte Configurar ESXi Dump Collector con ESXCLI . Puede instalar ESXi Dump Collector a través del medio de instalación de vCenter Server o utilizar ESXi Dump Collector que se incluye en vCenter Server Appliance. Después de que se complete la configuración, la memoria de VMkernel se envía al servidor de red especificado cuando el sistema encuentra un error crítico.

Configuración de seguridad

En la mayoría de las implementaciones, todos los hosts que aprovisione con vSphere Auto Deploy deberán tener la misma configuración de seguridad. Puede, por ejemplo, configurar el firewall para que permita el acceso de determinados servicios al sistema de ESXi, establecer la configuración de seguridad, la configuración de usuario y la configuración del grupo de usuarios para el host de referencia con los comandos vCLI o vSphere Web Client. La configuración de seguridad incluye la configuración compartida de acceso de usuarios para todos los hosts. Puede lograr un acceso de usuarios unificado mediante la configuración de su host de referencia para la utilización de Active Directory. Consulte la documentación sobre *seguridad de vSphere*.

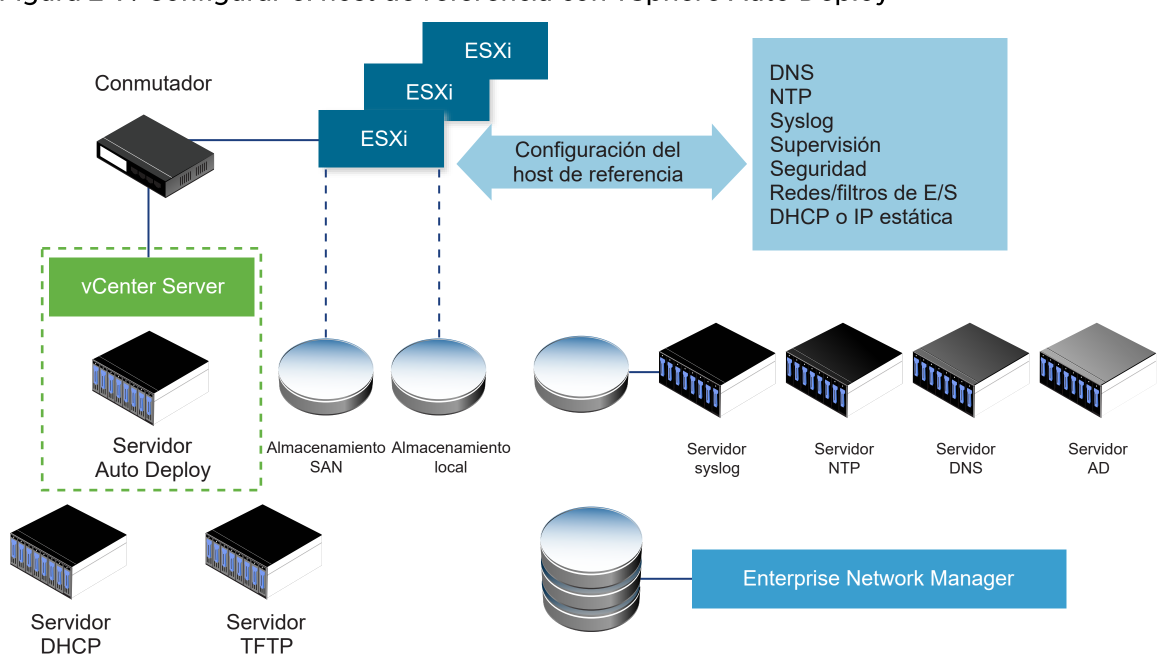
Nota Si configura Active Directory utilizando perfiles de host, las contraseñas no poseen protección. Utilice vSphere Authentication Service para configurar Active Directory para evitar la exposición de la contraseña de Active Directory.

Configuración de conexión de redes y almacenamiento

Si reserva un conjunto de recursos de conexión de redes y almacenamiento para la utilización por parte de los hosts aprovisionados con vSphere Auto Deploy, puede configurar su host de referencia para utilizar dichos recursos.

En implementaciones muy grandes, la configuración del host de referencia admite un Enterprise Network Manager, que recolecta toda la información proveniente de diferentes servicios de supervisión que se ejecutan en su entorno.

Figura 2-7. Configurar el host de referencia con vSphere Auto Deploy



Opciones para la configuración de un host de referencia de vSphere Auto Deploy explica cómo realizar esta configuración.

Vea el vídeo Hosts de referencia con Auto Deploy para obtener información sobre la configuración del host de referencia:

Configurar los hosts de referencia con vSphere Auto Deploy (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_fpu1jo7j/uiConfId/49694343/)

Opciones para la configuración de un host de referencia de vSphere Auto Deploy

Puede configurar un host de referencia usando vSphere Web Client, VCLI o perfiles de host.

Para configurar un host de referencia, puede utilizar el enfoque que mejor se adapte a sus necesidades.

vSphere Web Client

vSphere Web Client admite la configuración de la conexión de red, almacenamiento, seguridad y muchos otros aspectos de un host ESXi. Configure su entorno y cree un perfil de host desde el host de referencia para su uso por parte de vSphere Auto Deploy.

vSphere Command-Line Interface

Puede utilizar los comandos vCLI para configurar varios aspectos de su host. vCLI es adecuado para la configuración de muchos de los servicios del entorno de vSphere. Los comandos son, entre otros, `vicfg-ntp` para configurar un servidor NTP, `esxcli system syslog` para configurar un servidor syslog, `esxcli network route` para agregar rutas y configurar la ruta predeterminada, y `esxcli system coredump` para configurar ESXi Dump Collector.

Función Perfiles de host

La práctica recomendada es configurar un host con vSphere Web Client o vCLI y crear un perfil de host desde dicho host. Si lo prefiere, no obstante, puede utilizar la función Perfiles de host en vSphere Web Client y guardar dicho perfil de host.

vSphere Auto Deploy aplica todas las configuraciones comunes del perfil de host a todos los hosts de destino. Si configura el perfil de host para solicitar la entrada del usuario, todos los hosts aprovisionados con dicho perfil de host aparecen en el modo de mantenimiento. Debe volver a aplicar el perfil de host o restablecer las personalizaciones del host para solicitar información específica del host.

Configurar ESXi Dump Collector con ESXCLI

Los hosts aprovisionados con vSphere Auto Deploy no cuentan con un disco local para almacenar los volcados de memoria de núcleo. Puede configurar ESXi Dump Collector mediante los comandos ESXCLI para mantener los volcados de núcleos en un servidor de red con la finalidad de usarlos durante las operaciones de depuración.

Un volcado de núcleo es el estado de la memoria de trabajo en caso de que se produzca un error en el host. De forma predeterminada, los volcados de núcleos se guardan en el disco local. ESXi Dump Collector es especialmente útil para vSphere Auto Deploy, pero es compatible con cualquier host ESXi. ESXi Dump Collector admite otras opciones de personalización, incluido el envío de volcados de núcleos al disco local, y se incluye con el nodo de administración de vCenter Server.

Si va a usar IPv6 y el host ESXi y ESXi Dump Collector se encuentran en el mismo vínculo local, ambos pueden usar direcciones IPv6 de vínculo de alcance local o direcciones IPv6 de alcance global.

Si va a usar IPv6 y ESXi y ESXi Dump Collector se encuentran en hosts diferentes, ambos requieren direcciones IPv6 de alcance global. El tráfico se enruta por medio de la puerta de enlace IPv6 predeterminada.

Requisitos previos

Instale vCLI si quiere configurar el host para que use ESXi Dump Collector. En situaciones de solución de problemas, puede usar ESXCLI en ESXi Shell en su lugar.

Procedimiento

1 Configure un sistema ESXi para que use ESXi Dump Collector; para ello, ejecute `esxcli system coredump` en la instancia de ESXi Shell local o use vCLI.

```
 esxcli system coredump network set --interface-name vmk0    --server-ip 10xx.xx.xx.xx --
server-port 6500
```

   Debe especificar una dirección IP y la NIC de VMkernel, además de un puerto opcional del servidor al cual se deben enviar los volcados de núcleos. Puede usar una dirección IPv4 o IPv6. Si configura un sistema ESXi que se ejecuta en una máquina virtual que usa un conmutador estándar de vSphere, debe seleccionar un puerto de VMkernel que esté en modo promiscuo.

2 Habilite ESXi Dump Collector.

```
esxcli system coredump network set --enable true
```

3 (opcional) Compruebe que ESXi Dump Collector esté configurado correctamente.

```
esxcli system coredump network check
```

Resultados

El host en el que ha configurado ESXi Dump Collector está configurado para enviar los volcados de núcleos al servidor indicado mediante la NIC de VMkernel y el puerto opcional especificados.

Pasos siguientes

- Cree una regla que aplique el perfil de host a todos los hosts que desea aprovisionar con la configuración especificada en el host de referencia. Para escribir una regla en una sesión de PowerCLI, consulte Escribir una regla y asignar un perfil de host a hosts.
- Si los hosts ya se aprovisionaron con vSphere Auto Deploy, ejecute la prueba y repare las operaciones de cumplimiento en una sesión de PowerCLI. Para eso, consulte Probar y reparar cumplimiento de reglas .
- Encienda los hosts no aprovisionados para aprovisionarlos con el nuevo perfil de host.

Configurar ESXi Dump Collector desde la función de perfiles de host de vSphere Web Client

Los hosts aprovisionados con vSphere Auto Deploy no cuentan con un disco local para almacenar los volcados de memoria de núcleo. Puede configurar un host de referencia para usar ESXi Dump Collector desde la función de perfiles de host de vSphere Web Client.

La práctica recomendada es usar ESXi Dump Collector con el comando `esxcli system coredump` y guardar el perfil de host. Para obtener más información, consulte Configurar ESXi Dump Collector con ESXCLI .

Requisitos previos

- Compruebe que haya creado el perfil de host donde desea configurar una directiva de volcado de núcleo. Para obtener más información sobre la forma de crear un perfil de host, consulte la documentación de *Perfiles de host de vSphere*.
- Compruebe que al menos una partición disponga de capacidad de almacenamiento suficiente para los volcados de núcleos de varios hosts aprovisionados con vSphere Auto Deploy.

Procedimiento

1. En vSphere Web Client, haga clic en **Directivas y perfiles** y seleccione **Perfiles de host**.
2. Haga clic con el botón derecho en el perfil de host que desea modificar y seleccione **Editar configuración**.
3. Conserve el nombre y la descripción sin cambios, y haga clic en **Siguiente**.
4. En la página Editar perfil de host del asistente, seleccione **Configuración de redes > Configuración de volcados de núcleos de red**.
5. Active la casilla **Habilitado**.
6. Especifique la NIC del host que se debe usar, la IP del servidor de volcados de núcleos de red y el puerto del servidor de volcados de núcleos de red.
7. Haga clic en **Finalizar** para guardar la configuración del perfil de host.

Pasos siguientes

- Cree una regla que aplique el perfil de host a todos los hosts que desea aprovisionar con la configuración especificada en el host de referencia. Para escribir una regla en una sesión de PowerCLI, consulte Escribir una regla y asignar un perfil de host a hosts.
- Si los hosts ya se aprovisionaron con vSphere Auto Deploy, ejecute la prueba y repare las operaciones de cumplimiento en una sesión de PowerCLI. Para eso, consulte Probar y reparar cumplimiento de reglas .
- Encienda los hosts no aprovisionados para aprovisionarlos con el nuevo perfil de host.

Configurar Syslog desde la función de perfiles de host de vSphere Web Client

Por lo general, los hosts aprovisionados con vSphere Auto Deploy no cuentan con almacenamiento local suficiente para guardar los registros del sistema. Puede especificar un servidor remoto de Syslog para esos hosts. Para ello, debe configurar un host de referencia, guardar el perfil de host y aplicar dicho perfil de host a los demás hosts según sea necesario.

La práctica recomendada es configurar el servidor syslog en el host de referencia con vSphere Web Client o con el comando `esxcli system syslog` y guardar el perfil de host. También puede configurar syslog desde la función de perfiles de host de vSphere Web Client.

Requisitos previos

- Si va a usar un host de Syslog remoto, configure ese host antes de personalizar los perfiles de host.
- Compruebe que tiene acceso a vSphere Web Client y que puede conectarse al sistema vCenter Server.

Procedimiento

1. En vSphere Web Client, haga clic en **Directivas y perfiles** y seleccione **Perfiles de host**.
2. (opcional) Si no existe ningún host de referencia en el entorno, haga clic en el icono **Extraer perfil de host** para crear un perfil de host.
3. Haga clic con el botón derecho en el perfil de host que desea modificar y seleccione **Editar configuración**.
4. Conserve el nombre y la descripción sin cambios, y haga clic en **Siguiente**.
5. En la página Editar perfil de host del asistente, seleccione **Opciones de configuración avanzadas > Opciones avanzadas > Opciones de configuración avanzadas**.

   Puede seleccionar subperfiles específicos y editar la configuración de syslog.
6. Si va a configurar un host ESXi 5.0 que no tenía un servidor syslog configurado previamente, debe crear una opción de configuración avanzada.
   a. Haga clic en el icono **Agregar subperfil**.
   b. Seleccione las **Opciones de configuración avanzadas** del nuevo subperfil en la parte superior de la lista.

c Desde la lista desplegable **Opción avanzada**, seleccione **Configurar una opción fija**.

d Especifique Syslog.global.loghost como la opción y el host como el valor.

Si va a configurar un host ESXi versión 5.1 o superior, o un host ESXi 5.0 que tiene syslog configurado, la opción Syslog.global.loghost ya aparece en la lista de opciones avanzadas.

7 Haga clic en **Finalizar** para guardar la configuración del perfil de host.

Pasos siguientes

- Cree una regla que aplique el perfil de host a todos los hosts que desea aprovisionar con la configuración especificada en el host de referencia. Para escribir una regla en una sesión de PowerCLI, consulte Escribir una regla y asignar un perfil de host a hosts.
- Si los hosts ya se aprovisionaron con vSphere Auto Deploy, ejecute la prueba y repare las operaciones de cumplimiento en una sesión de PowerCLI. Para eso, consulte Probar y reparar cumplimiento de reglas .
- Encienda los hosts no aprovisionados para aprovisionarlos con el nuevo perfil de host.

Habilitar el cliente NTP en un host de referencia de vSphere Web Client

Al recopilar información de generación de registros en entornos grandes, deberá asegurarse de que las horas de los registros se encuentren coordinadas. Puede configurar el host de referencia para usar el servidor NTP en el entorno, extraer el perfil de host y crear una regla de vSphere Auto Deploy para aplicarla a los demás hosts.

Procedimiento

1 En el navegador de vSphere Web Client, desplácese hasta el host que desea utilizar como host de referencia.

2 Seleccione la pestaña **Administrar** y haga clic en **Configuración**.

3 En **Sistema**, seleccione **Configuración de hora** y haga clic en **Editar**.

4 Seleccione el botón de opción **Usar protocolo de hora de red (Habilitar el cliente NTP)**.

Esta opción sincroniza la fecha y hora del host con un servidor NTP. El servicio NTP en el host toma periódicamente la fecha y la hora del servidor NTP.

5 Desde la lista desplegable **Directiva de inicio del servicio NTP**, seleccione **Iniciar y detener con el host**.

6 En el cuadro de texto **Servidores NTP**, escriba las direcciones IP o los nombres de host de los servidores NTP que se desea usar.

7 Haga clic en **Aceptar**.

Pasos siguientes

- Extraiga un perfil de host del host de referencia. Consulte la documentación sobre *perfiles de host*.

- Cree una regla que aplique el perfil de host a todos los hosts que desea aprovisionar con la configuración especificada en el host de referencia. Para escribir una regla en una sesión de PowerCLI, consulte Escribir una regla y asignar un perfil de host a hosts.

Configurar las redes para los hosts vSphere Auto Deploy en vSphere Web Client

Puede configurar redes para el host de referencia de vSphere Auto Deploy y aplicar el perfil de host a todos los demás hosts a fin de garantizar un entorno de red completamente funcional.

Requisitos previos

Use vSphere Auto Deploy para aprovisionar el host que desea utilizar como host de referencia con una imagen de ESXi.

Procedimiento

1. En el navegador de vSphere Web Client, desplácese hasta el host que desea utilizar como host de referencia.
2. Seleccione la pestaña **Administrar** y luego **Redes**.
3. Realice la configuración de redes.

   Si usa conmutadores virtuales y no vSphere Distributed Switch, no agregue otras NIC de VMkernel a vSwitch0.
4. Después de configurar el host de referencia, reinicie el sistema para comprobar que vmk0 esté conectado a la red de administración.
5. Si no existen perfiles de host para su host de referencia, cree un perfil de host.

Pasos siguientes

- Cree una regla que aplique el perfil de host a todos los hosts que desea aprovisionar con la configuración especificada en el host de referencia. Para escribir una regla en una sesión de PowerCLI, consulte Escribir una regla y asignar un perfil de host a hosts.
- Si los hosts ya se aprovisionaron con vSphere Auto Deploy, ejecute la prueba y repare las operaciones de cumplimiento en una sesión de PowerCLI. Para eso, consulte Probar y reparar cumplimiento de reglas .
- Encienda los hosts no aprovisionados para aprovisionarlos con el nuevo perfil de host.

Configurar un host de referencia para la creación automática de particiones

De manera predeterminada, vSphere Auto Deploy aprovisiona los hosts solo si hay una partición disponible en el host. La opción de creación automática de particiones crea un almacén de datos

de VMFS en el almacenamiento local del host. Puede configurar un host de referencia para crear particiones automáticamente de todos los hosts que aprovisione con vSphere Auto Deploy.

Precaución Si cambia el comportamiento predeterminado de creación automática de particiones, vSphere Auto Deploy sobrescribe las particiones existentes independientemente del contenido. Si activa esta opción, asegúrese de que no se produzca una pérdida de datos no intencionada.

A fin de garantizar que las unidades de estado sólido (SSD) locales permanezcan sin particionar durante la creación automática de particiones, deberá establecer el parámetro **`skipPartitioningSsds=TRUE`** en el host de referencia.

Para obtener más información sobre cómo evitar el formato de las unidades de estado sólido (SSD) durante la creación automática de particiones, consulte la documentación de *Almacenamiento de vSphere*.

Requisitos previos

- Use vSphere Auto Deploy para aprovisionar el host que desea utilizar como host de referencia con una imagen de ESXi.
- Compruebe que tiene acceso a vSphere Web Client y que puede conectarse al sistema vCenter Server.

Procedimiento

1. En el navegador de vSphere Web Client, desplácese hasta el host que desea utilizar como host de referencia.
2. Seleccione la pestaña **Administrar** y haga clic en **Configuración**.
3. En **Sistema**, seleccione **Configuración avanzada del sistema** y haga clic en **Editar**.
4. Desplácese a `VMkernel.Boot.autoPartition` y active la casilla **Habilitado**.
5. (opcional) Si no desea particionar las SSD locales, desplácese a `VMkernel.Boot.skipPartitioningSsds` y active la casilla **Habilitado**.
6. Haga clic en **Aceptar**.
7. Si no existen perfiles de host para su host de referencia, cree un perfil de host.

Resultados

La creación automática de particiones se realiza cuando se arrancan los hosts.

Pasos siguientes

- Utilice vSphere Auto Deploy para crear una regla que aplique el perfil de host de su host de referencia a todos los hosts inmediatamente al arrancar. Para crear una regla con vSphere Web Client, consulte Crear una regla de implementación. Para escribir una regla en una sesión de PowerCLI, consulte Escribir una regla y asignar un perfil de host a hosts.

Prácticas recomendadas y consideración de seguridad de vSphere Auto Deploy

Siga las prácticas recomendadas al instalar vSphere Auto Deploy y al utilizar vSphere Auto Deploy con otros componentes de vSphere. Configure la infraestructura altamente disponible de vSphere Auto Deploy en entornos de producción de gran tamaño o cuando utilice almacenamiento en caché sin estado. Siga todas las instrucciones de seguridad que seguiría en un entorno de arranque PXE y tenga en cuenta las recomendaciones de este capítulo.

vSphere Auto Deploy Best Practices

You can follow several vSphere Auto Deploy best practices, set up networking, configure vSphere HA, and otherwise optimize your environment for vSphere Auto Deploy.

See the VMware Knowledge Base for additional best practice information.

vSphere Auto Deploy and vSphere HA Best Practices

You can improve the availability of the virtual machines running on hosts provisioned with vSphere Auto Deploy by following best practices.

Some environments configure the hosts provisioned with vSphere Auto Deploy with a distributed switch or configure virtual machines running on the hosts with Auto Start Manager. In such environments, deploy the vCenter Server system so that its availability matches the availability of the vSphere Auto Deploy server. Several approaches are possible.

- Install vCenter Server on a Windows virtual machine or physical server or deploy the vCenter Server Appliance. Auto Deploy is deployed together with the vCenter Server system.
- Deploy the vCenter Server system on a virtual machine. Run the vCenter Server virtual machine in a vSphere HA enabled cluster and configure the virtual machine with a vSphere HA restart priority of high. Include two or more hosts in the cluster that are not managed by vSphere Auto Deploy and pin the vCenter Server virtual machine to these hosts by using a rule (vSphere HA DRS required VM to host rule). You can set up the rule and then disable DRS if you do not want to use DRS in the cluster. The greater the number of hosts that are not managed by vSphere Auto Deploy, the greater your resilience to host failures.

  Nota This approach is not suitable if you use Auto Start Manager. Auto Start Manager is not supported in a cluster enabled for vSphere HA.

vSphere Auto Deploy Networking Best Practices

Prevent networking problems by following vSphere Auto Deploy networking best practices.

vSphere Auto Deploy and IPv6

Because vSphere Auto Deploy takes advantage of the iPXE infrastructure, if the hosts that you plan to provision with vSphere Auto Deploy are with legacy BIOS, the vSphere Auto Deploy server must have an IPv4 address. PXE booting with legacy BIOS firmware is possible only over IPv4. PXE booting with UEFI firmware is possible with either IPv4 or IPv6.

IP Address Allocation

Use DHCP reservations for address allocation. Fixed IP addresses are supported by the host customization mechanism, but providing input for each host is not recommended.

VLAN Considerations

Use vSphere Auto Deploy in environments that do not use VLANs.

If you intend to use vSphere Auto Deploy in an environment that uses VLANs, make sure that the hosts that you want to provision can reach the DHCP server. How hosts are assigned to a VLAN depends on the setup at your site. The VLAN ID might be assigned by the switch or the router, or might be set in the host's BIOS or through the host profile. Contact your network administrator to determine the steps for allowing hosts to reach the DHCP server.

vSphere Auto Deploy and VMware Tools Best Practices

When you provision hosts with vSphere Auto Deploy, you can select an image profile that includes VMware Tools, or select the smaller image associated with the image profile that does not contain VMware Tools.

You can download two image profiles from the VMware download site.

- `xxxxx-standard`: An image profile that includes the VMware Tools binaries, required by the guest operating system running inside a virtual machine. The image is usually named esxi-*version*-*xxxxx*-standard.
- `xxxxx-no-tools`: An image profile that does not include the VMware Tools binaries. This image profile is usually smaller has a lower memory overhead, and boots faster in a PXE-boot environment. This image is usually named esxi-*version*-*xxxxx*-no-tools.

With vSphere 5.0 Update 1 and later, you can deploy ESXi using either image profile.

- If the network boot time is of no concern, and your environment has sufficient extra memory and storage overhead, use the image that includes VMware Tools.
- If you find the network boot time too slow when using the standard image, or if you want to save some space on the hosts, you can use the image profile that does not include VMware Tools, and place the VMware Tools binaries on shared storage. See, Aprovisionar hosts ESXi mediante un perfil de imagen sin VMware Tools.

vSphere Auto Deploy Load Management Best Practices

Simultaneously booting large numbers of hosts places a significant load on the vSphere Auto Deploy server. Because vSphere Auto Deploy is a Web server at its core, you can use existing Web server scaling technologies to help distribute the load. For example, one or more caching reverse proxy servers can be used with vSphere Auto Deploy. The reverse proxies serve up the static files that make up the majority of an ESXi boot image. Configure the reverse proxy to cache static content and pass all requests through to the vSphere Auto Deploy server. For more information, watch the video "Using Reverse Web Proxy Servers for vSphere Auto Deploy Scalability":

Using Reverse Web Proxy Servers for vSphere Auto Deploy Scalability

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_9rzporg9/uiConfId/49694343/)

Use multiple TFTP servers to point to different proxy servers. Use one TFTP server for each reverse proxy server. After that, set up the DHCP server to send different hosts to different TFTP servers.

When you boot the hosts, the DHCP server redirects them to different TFTP servers. Each TFTP server redirects hosts to a different server, either the vSphere Auto Deploy server or a reverse proxy server, significantly reducing the load on the vSphere Auto Deploy server.

After a massive power outage, bring up the hosts on a per-cluster basis. If you bring multiple clusters online simultaneously, the vSphere Auto Deploy server might experience CPU bottlenecks. All hosts might come up after a delay. The bottleneck is less severe if you set up the reverse proxy.

vSphere Auto Deploy Logging and Troubleshooting Best Practices

To resolve problems that you encounter with vSphere Auto Deploy, use the vSphere Auto Deploy logging information from the vSphere Web Client and set up your environment to send logging information and core dumps to remote hosts.

vSphere Auto Deploy Logs

Download the vSphere Auto Deploy logs by going to the vSphere Auto Deploy page in the vSphere Web Client. See, Descargar registros de vSphere Auto Deploy.

Setting Up Syslog

Set up a remote syslog server. See the *vCenter Server and Host Management* documentation for syslog server configuration information. Configure the first host you boot to use the remote syslog server and apply that host's host profile to all other target hosts. Optionally, install and use the vSphere Syslog Collector, a vCenter Server support tool that provides a unified architecture for system logging, enables network logging, and lets you combine logs from multiple hosts.

Setting Up ESXi Dump Collector

Hosts provisioned with vSphere Auto Deploy do not have a local disk to store core dumps on. Install ESXi Dump Collector and set up your first host so that all core dumps are directed to ESXi Dump Collector, and apply the host profile from that host to all other hosts. See Configurar ESXi Dump Collector con ESXCLI .

Using vSphere Auto Deploy in a Production Environment

When you move from a proof of concept setup to a production environment, take care to make the environment resilient.

- Protect the vSphere Auto Deploy server. See vSphere Auto Deploy and vSphere HA Best Practices.
- Protect all other servers in your environment, including the DHCP server and the TFTP server.

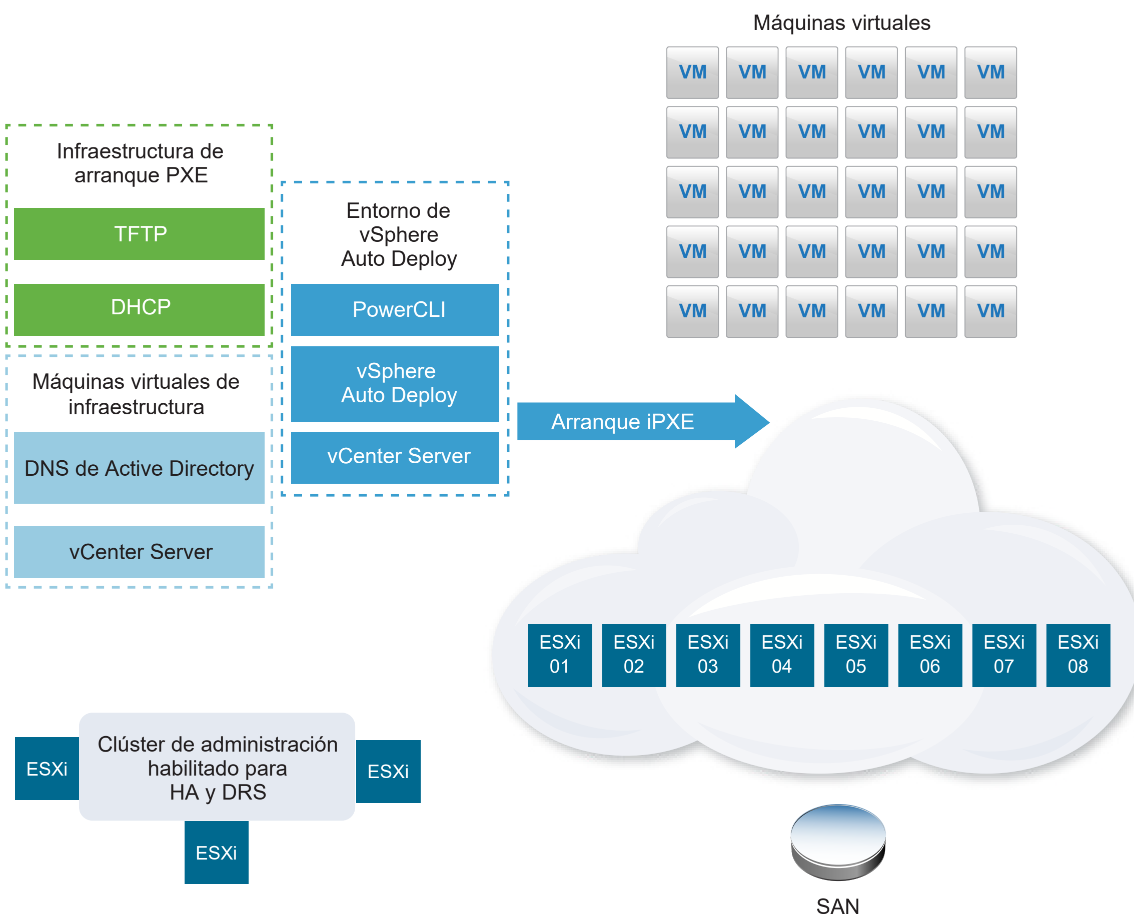
- Follow VMware security guidelines, including those outlined in Consideraciones de seguridad de vSphere Auto Deploy.

Set Up Highly Available vSphere Auto Deploy Infrastructure

In many production situations, a highly available vSphere Auto Deploy infrastructure is required to prevent data loss. Such infrastructure is also a prerequisite for using vSphere Auto Deploy with stateless caching.

Highly Available vSphere Auto Deploy Infrastructure (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_3gn1maf3/uiConfId/49694343/)

Figura 2-8. Highly Available vSphere Auto Deploy Infrastructure



Requisitos previos

For the management cluster, install ESXi on three hosts. Do not provision the management cluster hosts with vSphere Auto Deploy.

Watch the video "Highly Available vSphere Auto Deploy Infrastructure" for information about the implementation of a highly available vSphere Auto Deploy infrastructure:

Procedimiento

1. Enable vSphere HA and vSphere DRS on the management cluster.
2. Set up the following virtual machines on the management cluster.

Infrastructure Component	Description
PXE boot infrastructure	TFTP and DHCP servers.
Infrastructure VM	Active Directory, DNS, vCenter Server.
vSphere Auto Deploy environment	PowerCLI, vSphere Auto Deploy server, vCenter Server. Set up this environment on a single virtual machine or on three separate virtual machines in production systems.

   The vCenter Server on the infrastructure virtual machine differs from the vCenter Server in the vSphere Auto Deploy environment.

3. Set up vSphere Auto Deploy to provision other hosts as needed.

   Because the components on the management cluster are protected with vSphere HA, high availability is supported.

Consideraciones de seguridad de vSphere Auto Deploy

Cuando utilice vSphere Auto Deploy, preste especial atención a la seguridad de redes, a la seguridad de la imagen de arranque y a la posible exposición de la contraseña en los perfiles de host para proteger su entorno.

Seguridad de redes

Asegure su red igual que si se tratara de cualquier otro método de implementación basado en PXE. vSphere Auto Deploy transfiere datos por SSL para evitar interferencias accidentales e intromisiones. Sin embargo, la autenticidad del cliente o del servidor Auto Deploy no se comprueba durante un arranque PXE.

Puede reducir ampliamente el riesgo de seguridad de Auto Deploy aislando por completo la red donde se utiliza Auto Deploy.

Imagen de arranque y seguridad de perfil de host

La imagen de arranque que descarga el servidor vSphere Auto Deploy en una máquina puede tener los siguientes componentes.

- Los paquetes de VIB que componen el perfil de imagen se incluyen siempre en la imagen de arranque.
- El perfil de host y la personalización del host se incluyen en la imagen de arranque si las reglas de Auto Deploy se configuran para aprovisionar el host con un perfil o una personalización del host.
  - La contraseña de administrador (raíz) y las contraseñas de usuario que se incluyen en el perfil de host y en la personalización de host están cifradas con hash SHA-512.

  - Cualquier otra contraseña asociada a los perfiles quedará excluida. Si configura Active Directory utilizando perfiles de host, las contraseñas no poseen protección.

    Utilice vSphere Authentication Proxy para evitar la exposición de las contraseñas de Active Directory. Si configura Active Directory utilizando perfiles de host, las contraseñas no están protegidas.

- El certificado y la clave SSL públicas y privadas del host se incluyen en la imagen de arranque.

Usar el perfil de host de configuración de alias de dispositivo

En vSphere 5.5 y posterior, puede asignar un dispositivo (dirección de bus) de forma persistente a un nombre de dispositivo (alias). Puede modificar la asignación mediante el perfil de host de configuración de alias de dispositivo. El uso de la asignación persistente puede ayudar a evitar advertencias de cumplimiento para los hosts sin estado y también es útil para los hosts con estado.

El perfil de host de configuración de alias de dispositivo se selecciona de forma predeterminada, lo que implica que los alias se asignan a cada dispositivo. Por ejemplo, si un host no reconoce una de las NIC durante el proceso de arranque, los alias de NIC ya no se modifican. Esto puede ser de ayuda para la administración generada por script y también si aplica un perfil de host desde un host de referencia.

Nota Para evitar errores, no deshabilite ni edite el perfil de host de configuración de alias de dispositivo.

Para asegurarse de que la nomenclatura de los dispositivos sea uniforme, persistente y estable en todos los hosts, utilice el perfil de alias de dispositivo solo con hosts homogéneos. Estos son hosts configurados de forma idéntica con las mismas tarjetas de red y de almacenamiento en el bus PCI.

Nota Lleve siempre el BIOS al nivel más reciente. En el caso de sistemas con versiones del BIOS anteriores, es posible que el BIOS no proporcione información de ubicación precisa para los dispositivos en la tarjeta. En estos casos, ESXi aplica heurística para mantener el alias estable, incluso para estos dispositivos. Es posible que esto no funcione en todas las situaciones, por ejemplo, si los cambios se realizan en la configuración del BIOS o si los dispositivos tienen errores.

Errores de cumplimiento de la configuración de alias de dispositivo

En el caso de los hosts que no son completamente homogéneos (por ejemplo, los hosts que contienen tarjetas PCI distintas o tienen niveles de BIOS diferentes), si aplica el perfil de host desde un host de referencia, es posible que la comprobación de cumplimiento genere un error de cumplimiento. La comprobación de cumplimiento omite los dispositivos adicionales del host que no estaban en el host de referencia. Seleccione el host con menos dispositivos como el host de referencia.

Si la comprobación de cumplimiento muestra que los hosts no son totalmente homogéneos, será necesario modificar el propio hardware para corregir el error de cumplimiento.

Si el error de cumplimiento muestra que los alias de dispositivo (por ejemplo, nombres como vmhba3) son distintos de los que figuran en el host de referencia, es posible realizar la corrección.

- Para corregir un host que no está aprovisionado con vSphere Auto Deploy, realice la corrección del perfil de host y reinicie el host.
- Para corregir un host aprovisionado con vSphere Auto Deploy, vuelva a aprovisionar un host.

Actualizar sistemas para perfiles de alias de dispositivo

En versiones de ESXi anteriores a 5.5, el perfil de configuración de alias de dispositivo no existe. Tenga en cuenta los siguientes problemas cuando actualice desde versiones anteriores de ESXi a ESXi 5.5 y posteriores:

- En los hosts instalados, es decir, los que no están aprovisionados con vSphere Auto Deploy, debe actualizar el host ESXi para conservar los alias. Una vez actualizados, los alias permanecen estables siempre que el BIOS proporcione la información.
- Al actualizar un clúster de host ESXi aprovisionado con una imagen de vSphere Auto Deploy, los alias no cambian debido a que ESXi 5.5 usa el mismo algoritmo para generar alias que las versiones anteriores. Genere un nuevo perfil de host para el host de referencia. Este perfil de host incluye el perfil de configuración de alias de dispositivo. Configure vSphere Auto Deploy para aplicar el perfil de host del host de referencia a todos los demás hosts, para que la nomenclatura de dispositivos sea coherente en todo el clúster.
- Al actualizar un sistema, no actualice el BIOS, ya que esta acción podría cambiar los alias. La actualización del BIOS al nivel más reciente es más adecuada en el caso de una instalación nueva.

Aprovisionar hosts ESXi mediante un perfil de imagen sin VMware Tools

Cuando se aprovisionan hosts ESXi con vSphere Auto Deploy, se puede elegir aprovisionar el host mediante el perfil de imagen que no contiene binarios de VMware Tools. Generalmente, este perfil de imagen es de menor tamaño, posee menos sobrecarga de memoria y arranca más rápido en un entorno de arranque PXE.

Si al usar la imagen estándar encuentra que la red tarda demasiado en arrancar, o bien si desea guardar algo de espacio en los hosts, puede usar el perfil de imagen que no incluye VMware Tools y colocar los binarios de VMware Tools en un almacenamiento compartido.

Requisitos previos

Descargue el perfil de imagen `*xxxxx*-no-tools` del sitio de descarga de VMware.

Procedimiento

1 Arranque un host ESXi que no se aprovisionó con vSphere Auto Deploy.

2 Copie el directorio `/productLocker` desde el host ESXi hasta un almacenamiento compartido.

3 Cambie la variable *UserVars.ProductLockerLocation* para que apunte al directorio `/productLocker`.

   a En vSphere Web Client, seleccione el host de referencia y haga clic en la pestaña **Administrar**.

   b Seleccione **Configuración** y haga clic en **Configuración avanzada del sistema**.

   c Filtre la configuración para **`uservars`** y seleccione **UserVars.ProductLockerLocation**.

   d Haga clic en el icono de **lápiz** para editar la configuración para que apunte al almacenamiento compartido.

4 Cree un perfil de host desde el host de referencia.

5 Cree una regla de vSphere Auto Deploy que asigne el perfil de imagen *`xxxxx`*`-no-tools` y el perfil de host desde el host de referencia hasta todos los otros hosts.

6 Arranque sus host de destino con la regla para que elijan la ubicación del casillero del producto desde el host de referencia.

Descargar registros de vSphere Auto Deploy

Puede usar la información de registro de vSphere Auto Deploy de vSphere Web Client para solucionar los problemas que experimente con vSphere Auto Deploy.

Requisitos previos

Use vSphere Web Client para iniciar sesión en la instancia de vCenter Server con la que se ha registrado vSphere Auto Deploy.

Procedimiento

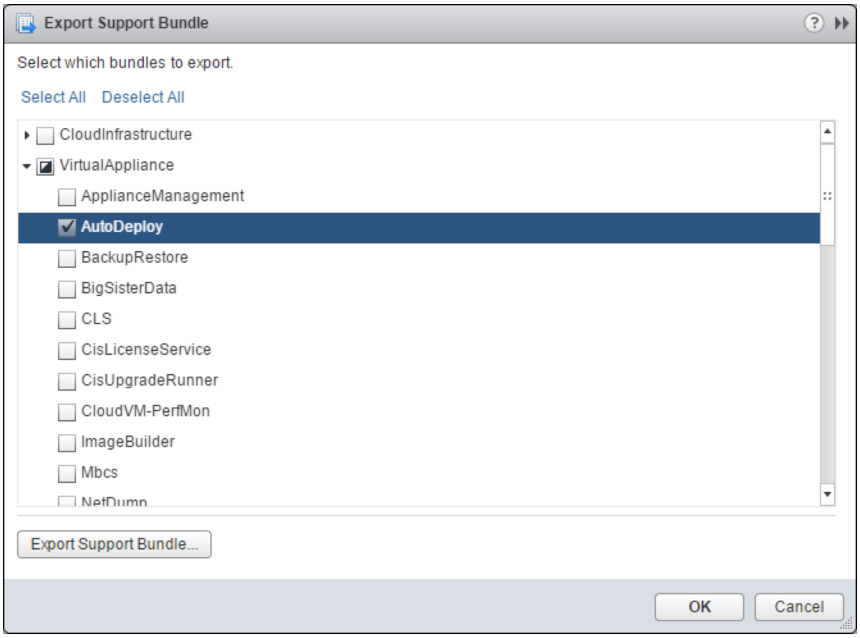
1 En **Administración**, seleccione **Implementación > Configuración del sistema**.

2 Haga clic en uno de los nodos para el que desea recuperar un paquete de soporte. El paquete de soporte contiene los registros de los servicios.

3 En el menú **Acciones**, seleccione la opción **Exportar paquetes de soporte...**

4 Seleccione solo **Dispositivo virtual > Auto Deploy**.

5 Haga clic en el botón **Exportar paquete de soporte...** para descargar los archivos de registro.



Configurar vSphere Auto Deploy y aprovisionar hosts con vSphere PowerCLI

En este escenario, se va a configurar un entorno de trabajo de vSphere Auto Deploy que incluya cuatro hosts. Creará reglas y aprovisionará dos de los hosts con un perfil de imagen, y aprovisionará a los dos hosts restantes con el mismo perfil de imagen y un perfil de host configurado para solicitar la entrada del usuario.

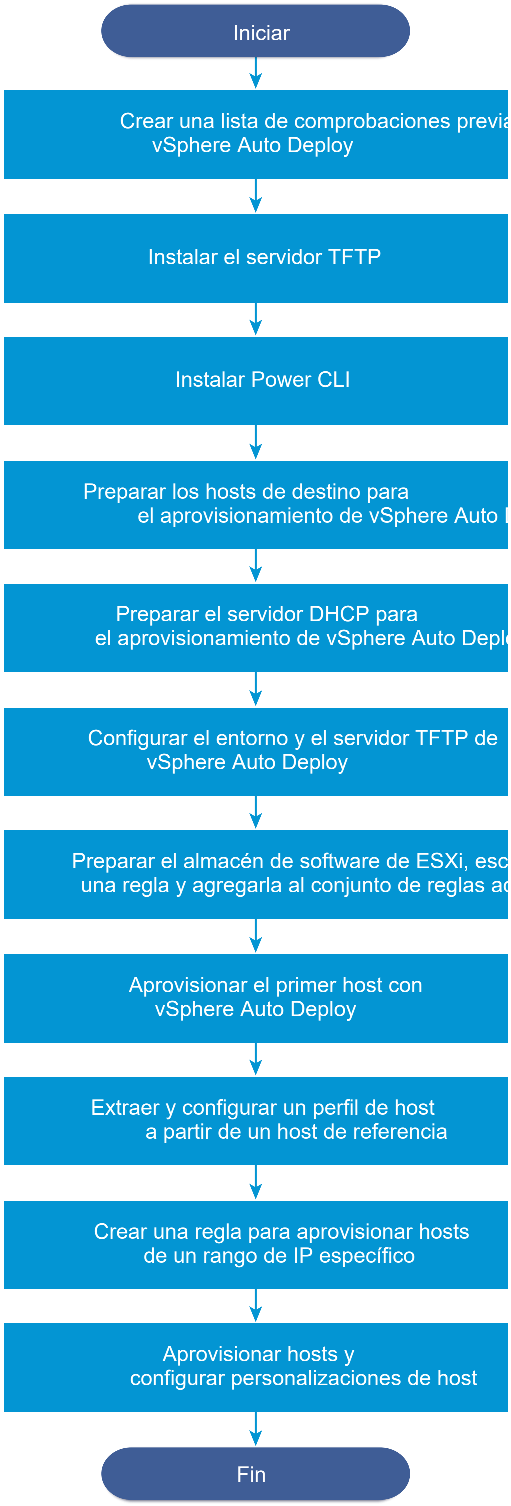
Este escenario le puede proporcionar la base para un entorno de producción. En las descripciones de las tareas se asume que va a utilizar una red común sin etiquetado de VLAN entre los hosts físicos y el resto de su entorno.

Para realizar las tareas de este escenario, deberá contar con los siguientes conocimientos y privilegios.

- Experiencia con vSphere (vCenter Server y ESXi).
- Conocimientos básicos sobre Microsoft PowerShell y PowerCLI.
- Derechos de administrador en los sistemas Windows y vCenter Server de destino.

Siga las tareas en el orden presentado en este escenario. Algunos pasos pueden realizarse en un orden diferente, pero el orden utilizado aquí limita las manipulaciones repetidas de algunos componentes.

Figura 2-9. Instalación y flujo de trabajo de aprovisionamiento de hosts de vSphere Auto Deploy



vSphere Auto Deploy aprovecha la infraestructura de iPXE; el arranque PXE con el firmware de BIOS heredado solo es posible en IPv4. Si los hosts que quiere aprovisionar con vSphere Auto Deploy presentan un BIOS heredado, el servidor vSphere Auto Deploy debe tener una dirección IPv4. El arranque PXE con firmware UEFI se puede realizar mediante IPv4 o IPv6.

Procedimiento

1 Lista de comprobación previa a la instalación de vSphere Auto Deploy

   Para poder iniciar las tareas en este escenario de vSphere Auto Deploy, primero debe asegurarse de que el entorno cumpla con los requisitos de hardware y software, y de contar con los permisos necesarios para los componentes que se incluyen en la configuración.

2 Instalar el servidor TFTP

   Para configurar una infraestructura de vSphere Auto Deploy, es necesario instalar un servidor TFTP en el entorno. vSphere Auto Deploy depende de un servidor TFTP para enviar una imagen de arranque a los hosts que aprovisiona.

3 Instalar PowerCLI

   Para poder administrar vSphere Auto Deploy mediante reglas creadas con cmdlets de PowerCLI, primero es necesario instalar PowerCLI.

4 Preparar los hosts de destino de vSphere Auto Deploy

   Es necesario configurar los parámetros del BIOS para los cuatro hosts y volver a confirmar la dirección MAC del dispositivo de red principal a fin de preparar los hosts de destino para el aprovisionamiento con vSphere Auto Deploy.

5 Preparar el servidor DHCP para el aprovisionamiento de vSphere Auto Deploy

   Cuando se preparan los hosts de destino de vSphere Auto Deploy, es necesario configurar el servidor DHCP de este escenario para proporcionar un archivo binario iPXE a cada host de destino.

6 Configure vSphere Auto Deploy y el entorno de TFTP en vSphere Web Client

   Después de preparar el servidor DHCP, debe iniciar el servicio vSphere Auto Deploy vCenter Server y configurar el servidor TFTP. Debe descargar un archivo ZIP de arranque TFTP del servidor vSphere Auto Deploy. El servidor FTP personalizado aloja las imágenes de arranque que proporciona vSphere Auto Deploy.

7 Preparar el almacén de software de ESXi y escribir una regla

   Después de configurar la infraestructura de vSphere Auto Deploy, es necesario agregar un almacén de software de ESXi, especificar un perfil de imagen, escribir una regla y agregarla al conjunto de reglas activo.

8 Aprovisionar el primer host con vSphere Auto Deploy

   Después de crear una regla y agregarla al conjunto de reglas activo, es posible aprovisionar el primer host y comprobar la ubicación de su vCenter Server para completar la verificación de aprovisionamiento de imagen de la instalación.

9 Extraer y configurar un perfil de host a partir de un host de referencia

Después de aprovisionar el primer host, es posible extraer y configurar un perfil de host que se puede usar para aplicar la misma configuración a otros hosts de destino. La configuración que varía en los distintos hosts, como la dirección IP estática, se puede administrar a través del mecanismo de personalización de host.

10 Crear una regla para aprovisionar hosts de un rango de IP específico

Después de crear un perfil de host a partir de un host de referencia, puede crear una regla para aplicar el perfil de imagen previamente verificado y el perfil de host extraído a hosts de destino en un rango de IP específico.

11 Aprovisionar hosts y configurar personalizaciones de host

Con la aplicación de la regla para aprovisionar hosts mediante un perfil de imagen y un perfil de host, es posible aprovisionar hosts de destino específicos. Si algún elemento del perfil de host está configurado para solicitar la intervención del usuario, el host se activa en modo de mantenimiento. Debe aplicar el perfil de host o comprobar el cumplimiento de host para que se le pida la información. El sistema asocia la personalización del host con el host.

Lista de comprobación previa a la instalación de vSphere Auto Deploy

Para poder iniciar las tareas en este escenario de vSphere Auto Deploy, primero debe asegurarse de que el entorno cumpla con los requisitos de hardware y software, y de contar con los permisos necesarios para los componentes que se incluyen en la configuración.

Tabla 2-18. Lista de verificación previa a la instalación

Software y hardware necesarios	Detalles
vCenter Server	El servidor vSphere Auto Deploy forma parte de vCenter Server. Debe habilitar e iniciar el servicio vSphere Auto Deploy en el sistema vCenter Server. Puede realizar muchas de las tareas de configuración iniciando sesión en vCenter Server. Consulte #unique_203.
Almacenamiento	El almacenamiento para los almacenes de datos NFS, iSCSI o Fibre Channel de ESXi, con servidores y matrices de almacenamiento que se configuran de manera tal que los servidores puedan detectar los LUN. ■ Una lista de las direcciones IP de destino para NFS o iSCSI. ■ Una lista con la información de los volúmenes de destino para NFS o iSCSI.

Tabla 2-18. Lista de verificación previa a la instalación (continuación)

Software y hardware necesarios	Detalles
Información del host (para cuatro hosts ESXi)	Una lista de las direcciones IP de destino para NFS o iSCSI. Una lista con la información de los volúmenes de destino para NFS o iSCSI. ■ La ruta predeterminada, la máscara de red y las direcciones IP de los servidores DNS principales y secundarios. ■ La dirección IP y la máscara de red de la red de administración principal de VMkernel. ■ La dirección IP y la máscara de red de las demás redes de VMkernel, como el almacenamiento, vSphere FT o VMware vMotion. vSphere Auto Deploy no sobrescribe las particiones existentes como opción predeterminada.
PowerCLI	Consulte Instalar PowerCLI.
Almacén de software de ESXi	La ubicación del almacén de software de ESXi en la página de descargas del sitio web de VMware. Se debe usar una URL para apuntar al perfil de imagen que está almacenado en esa ubicación o se debe descargar un archivo .zip que funcione con un almacén local. No descargue la imagen de ESXi.
servidor TFTP	El software del instalador para TFTP, como un servidor TFTP de WinAgents.
Servidor DHCP	El servidor DHCP se incluye en las versiones de vSphere compatibles con Windows Server.
Servidor DNS	Un servidor DNS en funcionamiento. Es necesario agregar entradas tanto en Zona directa (Registro A) como en Zona inversa (Registro PTR) para cada host de destino.

También se necesita información acerca de los privilegios de administrador para los servidores principales del entorno, incluidos el servidor de Active Directory, el servidor DNS, el servidor DHCP, el servidor NTP, etc.

Se debe tener control completo del dominio de difusión de la subred en la que se implementa la configuración. Asegúrese de que no haya otros servidores DHCP, DNS ni TFTP en esta subred.

Instalar el servidor TFTP

Para configurar una infraestructura de vSphere Auto Deploy, es necesario instalar un servidor TFTP en el entorno. vSphere Auto Deploy depende de un servidor TFTP para enviar una imagen de arranque a los hosts que aprovisiona.

Con esta tarea solo se instala el servidor TFTP. Después se descarga un archivo de configuración en el servidor. Consulte Configure vSphere Auto Deploy y el entorno de TFTP en vSphere Web Client.

Procedimiento

1. Descargue el servidor TFTP que prefiera en una ubicación que tenga acceso de red a su vCenter Server e instale el servidor.
2. Configure el directorio raíz TFTP, por ejemplo, `D:\TFTP_Root\`.

Pasos siguientes

Instale PowerCLI para administrar vSphere Auto Deploy con cmdlets de PowerCLI.

Instalar PowerCLI

Para poder administrar vSphere Auto Deploy mediante reglas creadas con cmdlets de PowerCLI, primero es necesario instalar PowerCLI.

Requisitos previos

- Para seleccionar una versión de PowerCLI compatible con su versión de ESXi, utilice la Matriz de interoperabilidad de productos VMware.
- Compruebe los requisitos del sistema para la versión de PowerCLI que seleccionó mediante la Matriz de compatibilidad en la página de inicio de PowerCLI para la versión de PowerCLI correspondiente.
- Abra PowerShell en su estación de trabajo.

Procedimiento

1. Descargue una versión de PowerCLI posterior a PowerCLI 6.5R1 de la página de inicio de PowerCLI.
2. Para instalar todos los módulos de PowerCLI, ejecute el comando: `Install-Module VMware.PowerCLI -Scope CurrentUser`. Como alternativa, puede instalar módulos de PowerCLI individuales si ejecuta el cmdlet `Install-Module` con el nombre del módulo.

   Si aparece una advertencia de que está instalando módulos de un repositorio que no es de confianza, presione **y** y luego presione **Intro** para confirmar la instalación.
3. (Opcional) Si necesita instalar PowerCLI sin conexión, descargue el archivo ZIP de PowerCLI de la página de inicio de PowerCLI y transfiera el archivo ZIP al equipo local.
   a. Compruebe la ruta del módulo PowerShell mediante el comando: `$env:PSModulePath`.
   b. Extraiga el contenido del archivo ZIP en una de las carpetas enumeradas.
   c. Desbloquee los archivos con los comandos `cd <path_to_powershell_modules_folder>` y `Get-ChildItem * -Recurse | Unblock-File`.

   Puede comprobar que el módulo de PowerCLI esté disponible mediante el comando `Get-Module -Name VMware.PowerCLI -ListAvailable`.

Pasos siguientes

Configure los parámetros de los hosts de destino con el fin de prepararlos para el aprovisionamiento con vSphere Auto Deploy.

Preparar los hosts de destino de vSphere Auto Deploy

Es necesario configurar los parámetros del BIOS para los cuatro hosts y volver a confirmar la dirección MAC del dispositivo de red principal a fin de preparar los hosts de destino para el aprovisionamiento con vSphere Auto Deploy.

Requisitos previos

Los hosts que se deseen aprovisionar con vSphere Auto Deploy deben cumplir con los requisitos para ESXi.

Consulte Requisitos de hardware de ESXi.

Procedimiento

1 Modifique la configuración del BIOS de cada uno de los cuatro hosts físicos para forzar el arranque de los hosts desde el dispositivo de red principal.

2 Vuelva a confirmar la dirección MAC del dispositivo de red principal.

Pasos siguientes

Configure el servidor DHCP para proporcionar a cada host de destino un archivo binario iPXE.

Preparar el servidor DHCP para el aprovisionamiento de vSphere Auto Deploy

Cuando se preparan los hosts de destino de vSphere Auto Deploy, es necesario configurar el servidor DHCP de este escenario para proporcionar un archivo binario iPXE a cada host de destino.

En el entorno de este escenario, se utiliza Active Directory con DNS y DHCP. El servidor DHCP se incluye en las versiones de vSphere compatibles con Windows Server.

Procedimiento

1 Inicie sesión en el servidor DHCP con privilegios de administrador.

2 Cree un ámbito DHCP para el intervalo de direcciones IP.

   a Haga clic en **Inicio > Configuración > Panel de control > Herramientas administrativas** y seleccione **DHCP**.

   b Desplácese hasta **DHCP >** ***hostname*** **> IPv4**.

   c Haga clic con el botón derecho en **IPv4** y seleccione **Nuevo ámbito**.

   d En la pantalla principal, haga clic en **Siguiente** y especifique un nombre y una descripción para el ámbito.

e Especifique un intervalo de direcciones IP y haga clic en **Siguiente**.

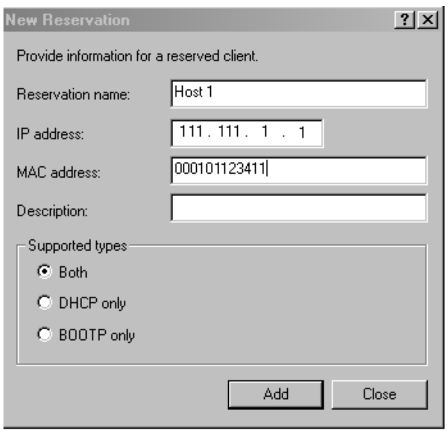
f Haga clic en **Siguiente** hasta llegar a la pantalla Configurar opciones DHCP. Allí, seleccione **No, configuraré esta opción más adelante**.

3 Cree una reserva de DHCP para cada host ESXi de destino.

a En la ventana DHCP, vaya a **DHCP** > ***hostname*** > **IPv4** > **Ámbito Auto Deploy** > **Reservas**.

b Haga clic con el botón derecho en **Reservas** y seleccione **Nueva reserva**.

c En la ventana Nueva reserva, especifique un nombre, una dirección IP y la dirección MAC de uno de los hosts. No incluya los dos puntos (:) en la dirección MAC.



d Repita el procedimiento para cada uno de los otros hosts.

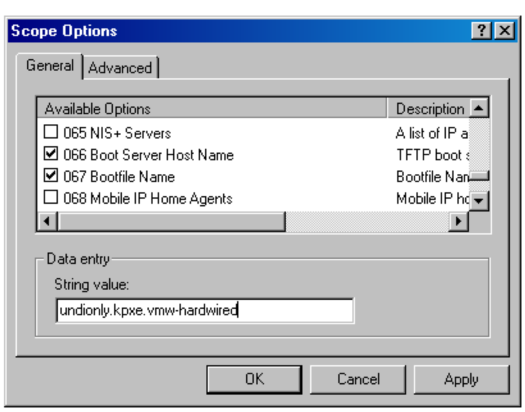
4 Configure el servidor DHCP para que apunte los hosts al servidor TFTP.

a En la ventana DHCP, vaya a **DHCP** > ***hostname*** > **IPv4** > **Ámbito Auto Deploy** > **Opciones de ámbito**.

b Haga clic con el botón derecho en **Opciones de ámbito** y elija **Configurar opciones**.

c En la ventana Opciones de ámbito, haga clic en la pestaña **General**.

d Haga clic en **066 Nombre de host de servidor de arranque** y escriba la dirección del servidor TFTP que instaló, en el campo Valor de cadena, debajo de Opciones disponibles.



e Haga clic en **067 Nombre de archivo de arranque** y escriba **`undionly.kpxe.vmw-hardwired`**.

El archivo binario iPXE `undionly.kpxe.vmw-hardwired` se utilizará para arrancar los hosts ESXi.

f Haga clic en **Aplicar** y, a continuación, en **Aceptar** para cerrar la ventana.

5 En la ventana DHCP, haga clic con el botón derecho en **DHCP >** ***hostname*** **> IPv4 > Ámbito > Activar** y haga clic en **Activar**.

6 Si va a utilizar Active Directory para DHCP y DNS, no cierre la sesión del servidor DHCP. De lo contrario, cierre sesión.

Pasos siguientes

Inicie el servicio vCenter Server de vSphere Auto Deploy y configure el servidor TFTP.

Configure vSphere Auto Deploy y el entorno de TFTP en vSphere Web Client

Después de preparar el servidor DHCP, debe iniciar el servicio vSphere Auto Deploy vCenter Server y configurar el servidor TFTP. Debe descargar un archivo ZIP de arranque TFTP del servidor vSphere Auto Deploy. El servidor FTP personalizado aloja las imágenes de arranque que proporciona vSphere Auto Deploy.

Procedimiento

1 Utilice vSphere Web Client para conectarse al sistema vCenter Server que administra el servidor vSphere Auto Deploy.

2 Cuando aparezca la advertencia de certificado, continúe hacia el sistema vCenter Server.

3 Inicie el servicio vSphere Auto Deploy.

a En la página de inicio de vSphere Web Client, haga clic en **Administración**.

b En **Configuración del sistema**, haga clic en **Servicios**.

c Seleccione **Auto Deploy**, haga clic en el menú **Acciones** y seleccione **Iniciar**.

En Windows, se puede deshabilitar el servicio vSphere Auto Deploy. Para habilitar el servicio, cambie el tipo de inicio del servicio vSphere Auto Deploy.

4 En el inventario, desplácese al sistema vCenter Server.

5 En la pestaña **Administrar**, seleccione **Configuración** y, a continuación, haga clic en **Auto Deploy**.

6 Haga clic en el vínculo **Descargar TFTP Boot Zip** para descargar el archivo de configuración de TFTP.

7 Guarde el archivo `Deploy-tftp.zip` en el directorio `TFTP_Root` que creó al instalar el servidor TFTP y descomprima el archivo.

Pasos siguientes

Agregue un almacén de software al inventario y utilice un perfil de imagen del almacén para crear una regla de aprovisionamiento de hosts.

Preparar el almacén de software de ESXi y escribir una regla

Después de configurar la infraestructura de vSphere Auto Deploy, es necesario agregar un almacén de software de ESXi, especificar un perfil de imagen, escribir una regla y agregarla al conjunto de reglas activo.

vSphere Auto Deploy aprovisiona hosts con perfiles de imagen donde se define el conjunto de VIB que se utiliza en un proceso de instalación de ESXi. Los perfiles de imágenes se almacenan en almacenes de software. Debe asegurarse de que esté disponible el perfil de imagen correcto antes de iniciar el aprovisionamiento de los hosts. Cuando se agrega un almacén de software a una sesión de PowerCLI, el almacén solo se encuentra disponible durante la sesión actual. No se mantiene de una sesión a otra.

Los pasos de esta tarea indican que se deben ejecutar cmdlets de PowerCLI. Para obtener información adicional sobre los cmdlets de vSphere Auto Deploy que se pueden ejecutar en una sesión de PowerCLI, consulte Descripción general de cmdlets de vSphere Auto Deploy PowerCLI.

Requisitos previos

Compruebe si puede acceder a los hosts ESXi que desea aprovisionar desde el sistema en el que se ejecuta PowerCLI.

Procedimiento

1 Inicie sesión como administrador en la consola del sistema Windows donde se instaló vCenter Server, ya sea de forma directa o mediante RDP.

   En esta tarea, se supone que PowerCLI se instaló en el sistema donde se ejecuta vCenter Server.

2 En una sesión de PowerCLI, ejecute el cmdlet `Connect-VIServer` para conectarse al sistema vCenter Server con el que se registró vSphere Auto Deploy.

   ```
   Connect-VIServer ipv4_address
   ```

   Es posible que el cmdlet devuelva una advertencia de certificado de servidor. En un entorno de producción, asegúrese de que no se produzca ningún problema de certificado de servidor. En un entorno de desarrollo, puede omitir la advertencia.

3 Introduzca las credenciales para vCenter Server.

4 Ejecute `Add-EsxSoftwareDepot` para agregar el almacén en línea a la sesión de PowerCLI.

   ```
   Add-EsxSoftwareDepot https://hostupdate.vmware.com/software/VUM/PRODUCTION/main/vmw-depot-index.xml
   ```

Se requiere agregar el almacén de software cada vez que se inicia una sesión nueva de PowerCLI.

5 Revise el contenido del almacén de software con el cmdlet `Get-EsxImageProfile` para comprobar si se agregó correctamente el almacén.

   El cmdlet devuelve información sobre todos los perfiles de imágenes en el almacén.

6 Ejecute el cmdlet `New-DeployRule` para crear una nueva regla.

```
New-DeployRule -Name "InitialBootRule" -Item ESXi-6.0.0-2494585-standard -AllHosts
```

   El cmdlet creará una regla para asignar el perfil de imagen especificado a todos los hosts del inventario.

7 Agregue la nueva regla al conjunto de reglas activo con la finalidad de que la regla esté disponible para el servidor vSphere Auto Deploy.

```
Add-DeployRule    -DeployRule "InitialBootRule"
```

Pasos siguientes

Aprovisione el primer host con vSphere Auto Deploy y revise su aprovisionamiento de imagen.

Aprovisionar el primer host con vSphere Auto Deploy

Después de crear una regla y agregarla al conjunto de reglas activo, es posible aprovisionar el primer host y comprobar la ubicación de su vCenter Server para completar la verificación de aprovisionamiento de imagen de la instalación.

Procedimiento

1 Abra una sesión de consola en el host físico que desee utilizar como el primer host ESXi de destino, arranque el host y busque mensajes que indiquen un arranque iPXE correcto.

   Durante el proceso de arranque, DHCP asigna una dirección IP al host. La dirección IP coincide con el nombre que especificó anteriormente en el servidor DNS. El host se pone en contacto con el servidor vSphere Auto Deploy y descarga los archivos binarios de ESXi desde la dirección URL de HTTP indicada en el archivo tramp de iPXE que descargó anteriormente al directorio TFTP_Root. Cada instancia de vSphere Auto Deploy produce un conjunto de archivos personalizado para el servidor TFTP.

2 Utilice vSphere Web Client para conectarse al sistema vCenter Server que administra el servidor vSphere Auto Deploy.

3 En la página de inicio de vSphere Web Client, haga clic en **Hosts y clústeres**.

4 Compruebe que el host recientemente aprovisionado se encuentre ahora en el inventario de vCenter Server en el nivel del centro de datos.

   De forma predeterminada, vSphere Auto Deploy agrega hosts en ese nivel cuando se completa el proceso de arranque.

Pasos siguientes

Extraiga un perfil de host del host y configúrelo para se requieran entradas del usuario.

Extraer y configurar un perfil de host a partir de un host de referencia

Después de aprovisionar el primer host, es posible extraer y configurar un perfil de host que se puede usar para aplicar la misma configuración a otros hosts de destino. La configuración que varía en los distintos hosts, como la dirección IP estática, se puede administrar a través del mecanismo de personalización de host.

vSphere Auto Deploy puede aprovisionar todos los hosts con el mismo perfil de host. vSphere Auto Deploy también puede utilizar la personalización de host para especificar información diferente para diversos hosts. Por ejemplo, si configura un puerto VMkernel para vMotion o para almacenamiento, puede especificar una dirección IP estática para el puerto mediante el mecanismo de personalización de host.

Procedimiento

1. Utilice vSphere Web Client para conectarse al sistema vCenter Server que administra el servidor vSphere Auto Deploy.
2. Haga clic en **Directivas y perfiles** y seleccione **Perfiles de host**.
3. Haga clic en **Extraer perfil de un host**.
4. En la página Seleccionar host del asistente, seleccione el host de referencia que configuró anteriormente y haga clic en **Siguiente**.
5. En la página Nombre y descripción del asistente, asigne el nombre ESXiGold al perfil, agregue una descripción y haga clic en **Siguiente**.
6. Revise la configuración del perfil de host y haga clic en **Finalizar**.
7. Haga clic con el botón derecho en el nuevo perfil de host ESXiGold y seleccione **Editar configuración**.
8. Conserve el nombre y la descripción sin cambios, y haga clic en **Siguiente**.
9. En la página Editar perfil de host del asistente, seleccione **Seguridad y servicios > Configuración de seguridad > Seguridad > Configuración de usuario > raíz**.
10. En **Directiva de contraseñas** en el panel derecho, seleccione **Configuración de contraseña introducida por el usuario**.
11. Haga clic en **Finalizar** para guardar la configuración del perfil de host.

Pasos siguientes

Cree una regla de vSphere Auto Deploy para aplicar el perfil de host a otros hosts ESXi.

Crear una regla para aprovisionar hosts de un rango de IP específico

Después de crear un perfil de host a partir de un host de referencia, puede crear una regla para aplicar el perfil de imagen previamente verificado y el perfil de host extraído a hosts de destino en un rango de IP específico.

Procedimiento

1 Inicie sesión con privilegios de administrador en la consola del sistema Windows en el cual está instalado vCenter Server, ya sea de forma directa o mediante RDP.

2 En una sesión de PowerCLI, ejecute el cmdlet `Connect-VIServer` para conectarse al sistema vCenter Server con el que se registró vSphere Auto Deploy.

```
Connect-VIServer ipv4_address
```

Es posible que el cmdlet devuelva una advertencia de certificado de servidor. En un entorno de producción, asegúrese de que no se produzca ningún problema de certificado de servidor. En un entorno de desarrollo, puede omitir la advertencia.

3 Ejecute `Add-EsxSoftwareDepot` para agregar el almacén en línea a la sesión de PowerCLI.

```
Add-EsxSoftwareDepot https://hostupdate.vmware.com/software/VUM/PRODUCTION/main/vmw-depot-index.xml
```

Se requiere agregar el almacén de software cada vez que se inicia una sesión nueva de PowerCLI.

4 (Requerido) Ejecute el cmdlet `Get-DeployRuleset` para ver las reglas en el conjunto de reglas activo.

5 Cree una regla para indicar a vSphere Auto Deploy que debe aprovisionar el conjunto de hosts de un rango de IP específico con el perfil de imagen anteriormente seleccionado y el perfil de host creado a partir del host de referencia.

```
New-DeployRule -name "Production01Rule" -item "image_profile",ESXiGold -Pattern "ipv4=IP_range"
```

6 Agregue la nueva regla al conjunto de reglas activo.

```
Add-DeployRule    -DeployRule "Production01Rule"
```

7 Ejecute el comando `Get-DeployRuleset` para comprobar el conjunto de reglas activo.

En PowerCLI, se muestra información similar a la del siguiente ejemplo.

```
Name:               Production01Rule
PatternList:        {ipv4=address_range}
ItemList:           {ESXi-version-XXXXXX-standard, Compute01, ESXiGold}
```

Pasos siguientes

Aprovisione los hosts y configure personalizaciones de host.

Aprovisionar hosts y configurar personalizaciones de host

Con la aplicación de la regla para aprovisionar hosts mediante un perfil de imagen y un perfil de host, es posible aprovisionar hosts de destino específicos. Si algún elemento del perfil de host está configurado para solicitar la intervención del usuario, el host se activa en modo de mantenimiento. Debe aplicar el perfil de host o comprobar el cumplimiento de host para que se le pida la información. El sistema asocia la personalización del host con el host.

Procedimiento

1 Arranque los hosts restantes.

   vSphere Auto Deploy arranca los hosts, aplica el perfil de host y agrega los hosts al inventario de vCenter Server. Los hosts permanecen en el modo de mantenimiento, dado que el perfil de host de referencia está configurado para solicitar la intervención del usuario para cada host.

2 Utilice vSphere Web Client para conectarse al sistema vCenter Server que administra el servidor vSphere Auto Deploy.

3 Haga clic en **Directivas y perfiles** y seleccione **Perfiles de host**.

4 Haga clic con el botón derecho en el perfil ESXiGold creado previamente y seleccione **Editar personalizaciones de host**.

5 Introduzca las personalizaciones de host requeridas y guárdelas.

6 Aplique el perfil de host a cada uno de los hosts y desactive el modo de mantenimiento de los hosts. Como alternativa, puede reiniciar cada host.

   Una vez finalizado el progreso de reinicio, todo los hosts están en ejecución con la imagen que especifica y utiliza la configuración del perfil de host de referencia. El clúster muestra que todos los hosts son totalmente compatibles.

Resultados

Ahora todos los hosts están configurados con información compartida a través del perfil de host de referencia y con la información específica del host a través del mecanismo de personalización de host. En el próximo arranque, los hosts recibirán toda la información de perfil de host, incluidos los datos específicos de cada host, y se iniciarán totalmente configurados y fuera del modo de mantenimiento.

Configurar ESXi

Estos temas proporcionan información sobre el uso de la interfaz de usuario de la consola directa y la configuración de los valores predeterminados de ESXi.

Configurar ESXi automáticamente

Cuando enciende el host ESXi por primera vez o después de restablecer los valores predeterminados de configuración, el host pasa a la fase de autoconfiguración. En esta fase se configuran dispositivos de red y de almacenamiento del sistema con opciones predeterminadas.

De manera predeterminada, el protocolo de configuración dinámica de host (DHCP) configura IP y todos los discos internos visibles que están en blanco se formatean con el sistema de archivos de la máquina virtual (VMFS). De este modo, las máquinas virtuales pueden almacenarse en los discos.

Acerca de la interfaz de ESXi de la consola directa

Use la consola directa para la configuración inicial y solución de problemas de ESXi.

Conecte un teclado y monitor al host para usar la consola directa. Una vez que el host concluye la fase de configuración automática, aparece la consola directa en el monitor. Puede examinar la configuración de red predeterminada y cambiar cualquier configuración que no sea compatible con el entorno de red.

Las operaciones clave disponibles en la consola directa incluyen:

- Configuración de hosts
- Configuración de acceso administrativo
- Solucionar problemas

También puede usar vSphere Web Client para administrar el host mediante vCenter Server.

Tabla 2-19. Buscar en la consola directa

Acción	Clave
Ver y cambiar la configuración	F2
Cambiar la interfaz de usuario a modo de alto contraste	F4
Apagar o reiniciar el host	F12
Ver el registro de VMkernel	Alt+F12
Cambiar a la consola del shell	Alt+F1
Cambiar a la interfaz de usuario de la consola directa	Alt+F2
Mover la selección entre campos	Teclas de flecha
Seleccionar un elemento de menú	Intro
Alternar un valor	Barra espaciadora

Tabla 2-19. Buscar en la consola directa (continuación)

Acción	Clave
Confirmar comandos sensibles, como restablecimiento de valores predeterminados de la configuración	F11
Guardar y salir	Intro
Salir sin guardar	Esc
Salir de registros del sistema	q

Configuración de la distribución del teclado para la consola directa

Puede configurar la distribución del teclado que desea usar con la consola directa.

Procedimiento

1 Desde la consola directa, seleccione **Configurar teclado** y presione Intro.
2 Seleccione la distribución que desea usar.
3 Presione la barra espaciadora para habilitar y desactivar las selecciones.
4 Presione Intro.

Crear un mensaje emergente de seguridad para la consola directa

Un banner de seguridad es un mensaje que se muestra en la pantalla **Principal** de la consola directa.

Procedimiento

1 Desde vSphere Web Client, conéctese a vCenter Server.
2 Seleccione el host en el inventario.
3 Haga clic en la pestaña **Administrar**.
4 Haga clic en **Configuración**.
5 En Sistema, seleccione **Configuración avanzada del sistema**.
6 Seleccione **Anotaciones**.
7 Haga clic en el icono de edición.
8 Introduzca un mensaje de seguridad.

Resultados

El mensaje se muestra en la pantalla **Principal** de la consola directa.

Redirigir la consola directa a un puerto serie

Para administrar de forma remota el host ESXi desde una consola serie, puede redirigir la consola directa hacia un puerto serie.

vSphere admite el tipo de terminal VT100 y el emulador de terminal PuTTy para ver la consola directa a través del puerto serie.

Puede redirigir la consola directa hacia un puerto serie de varias formas.

- Redireccionar la consola directa a un puerto serie mediante la configuración manual de las opciones de arranque

  Cuando se redirige la consola directa a un puerto serie mediante la configuración de opciones de arranque, el cambio no persiste en los arranques subsiguientes.

- Redirigir la consola directa a un puerto serie desde vSphere Web Client

  Puede administrar de forma remota el host ESXi desde una consola que esté conectada al puerto serie redirigiendo la consola directa a los puertos serie com1 o com2. Cuando se utiliza vSphere Web Client para redirigir la consola directa a un puerto serie, la opción de arranque que se configura continúa después de los arranques posteriores.

- Redireccionar la consola directa a un puerto serie en un host implementado con Auto Deploy

  Después de redireccionar la consola directa a un puerto serie, puede determinar que esa configuración forme parte del perfil de host que se conserva cuando se reaprovisiona el host con Auto Deploy.

Redireccionar la consola directa a un puerto serie mediante la configuración manual de las opciones de arranque

Cuando se redirige la consola directa a un puerto serie mediante la configuración de opciones de arranque, el cambio no persiste en los arranques subsiguientes.

Requisitos previos

Compruebe que el puerto serie no esté en uso para la generación de registros y la depuración serie.

Procedimiento

1 Inicie el host.

2 Cuando aparezca la ventana Cargando el hipervisor de VMware, presione las teclas Mayús + O para editar las opciones de arranque.

3 Deshabilite logPort y gdbPort en com1 y establezca tty2Port en com1 introduciendo las siguientes opciones de arranque:

```
"gdbPort=none logPort=none tty2Port=com1";
```

Para utilizar com2, reemplace `com1` por `com2`.

Resultados

La consola directa se redirecciona al puerto serie hasta que reinicie el host. Para redireccionar la consola directa para los arranque subsiguientes, consulte Redirigir la consola directa a un puerto serie desde vSphere Web Client

Redirigir la consola directa a un puerto serie desde vSphere Web Client

Puede administrar de forma remota el host ESXi desde una consola que esté conectada al puerto serie redirigiendo la consola directa a los puertos serie com1 o com2. Cuando se utiliza vSphere Web Client para redirigir la consola directa a un puerto serie, la opción de arranque que se configura continúa después de los arranques posteriores.

Requisitos previos

- Compruebe que puede acceder al host desde vSphere Web Client.
- Compruebe que el puerto serie no esté en uso para registro y depuración seriales o para shell ESX (tty1Port).

Procedimiento

1. Desde vSphere Web Client, conéctese a vCenter Server.
2. Seleccione el host en el inventario.
3. Haga clic en la pestaña **Administrar**.
4. Haga clic en **Configuración**.
5. En Sistema, seleccione **Configuración avanzada del sistema**.
6. Asegúrese de que los campos **VMkernel.Boot.logPort** y **VMkernel.Boot.gdbPort** no estén establecidos para usar el puerto com al que desea redirigir la consola directa.
7. Configure **VMkernel.Boot.tty2Port** al puerto serie para redireccionar la consola directa a: **`com1`** o **`com2`**.
8. Reinicie el host.

Resultados

Ahora puede administrar de forma remota el host ESXi desde una consola que esté conectada al puerto serie.

Redireccionar la consola directa a un puerto serie en un host implementado con Auto Deploy

Después de redireccionar la consola directa a un puerto serie, puede determinar que esa configuración forme parte del perfil de host que se conserva cuando se reaprovisiona el host con Auto Deploy.

Requisitos previos

El puerto serie no deberá estar en uso para el registro y la depuración en serie.

Procedimiento

1 Desde vSphere Web Client, conéctese a vCenter Server.
2 Seleccione el host en el inventario.
3 Haga clic en la pestaña **Administrar**.
4 Seleccione **Configuración**.
5 Seleccione **Configuración avanzada del sistema**.
6 Asegúrese de que los campos **VMkernel.Boot.logPort** y **VMkernel.Boot.gdbPort** no estén establecidos para usar el puerto com al que desea redirigir la consola directa.
7 Configure **VMkernel.Boot.tty2Port** al puerto serie para redireccionar la consola directa a: **`com1`** o **`com2`**.
8 Haga clic en **Aceptar**.
9 Guarde el perfil de host y conecte el host al perfil. Consulte la documentación de *Perfiles de host de vSphere*.

Resultados

La configuración para redireccionar la consola directa a un puerto serie es almacenada por vCenter Server y se conserva cuando se reaprovisiona el host con Auto Deploy.

Habilitar el acceso a ESXi Shell y SSH con la interfaz de usuario de la consola directa

Use la interfaz de usuario de la consola directa para habilitar ESXi Shell.

Procedimiento

1 En la interfaz de usuario de la consola directa, presione F2 para acceder al menú Personalización del sistema.
2 Seleccione **Opciones de solución de problemas** y presione Intro.
3 En el menú Opciones del modo de solución de problemas, seleccione un servicio para habilitar.
   - Habilitar ESXi Shell
   - Habilitar SSH
4 Presione Intro para habilitar el servicio.
5 (opcional) Establezca el tiempo de espera de ESXi Shell.

   De manera predeterminada, el tiempo de espera de ESXi Shell es 0 (deshabilitado).

La configuración del tiempo de espera de disponibilidad es la cantidad de minutos que pueden transcurrir antes de que deba iniciar sesión después de que se habilite ESXi Shell. Después del período de tiempo de espera, si no se ha iniciado sesión, el shell se deshabilita.

Nota Si inicia sesión y se agota el tiempo de espera, la sesión se mantiene activa. Sin embargo, ESXi Shell se deshabilitará, lo que impide que otros usuarios inicien sesión.

a En el menú Opciones del modo de solución de problemas, seleccione **Modificar tiempos de espera de SSH y ESXi Shell** y presione Intro.

b Introduzca el tiempo de espera de disponibilidad en minutos.

El tiempo de espera de disponibilidad es la cantidad de minutos que pueden transcurrir antes de que deba iniciar sesión después de que se habilite ESXi Shell.

c Presione Intro.

d Introduzca el tiempo de espera de inactividad.

El tiempo de inactividad es la cantidad de minutos que pueden transcurrir antes de que el usuario cierre sesión en sesiones interactivas inactivas. Los cambios en el tiempo de espera de inactividad se aplican la próxima vez que un usuario inicia sesión en ESXi Shell y no afectan las sesiones actuales.

6 Presione Esc hasta que vuelva al menú principal de la interfaz de usuario de la consola directa.

Administrar ESXi de forma remota

Puede utilizar VMware Host Client, vSphere Web Client y vCenter Server para administrar los hosts ESXi.

Para obtener instrucciones sobre cómo descargar e instalar vCenter Server y los componentes de vCenter Server, o sobre cómo descargar e implementar vCenter Server Appliance, consulte Capítulo 4 Instalar vCenter Server y Platform Services Controller en Windows e Capítulo 3 Implementar vCenter Server Appliance y el dispositivo de Platform Services Controller. Para obtener información sobre cómo instalar VMware Host Client, consulte *Administración de hosts de vSphere Single*.

Configurar la contraseña de la cuenta de administrador

Puede usar la consola directa para establecer la contraseña para la cuenta de administrador (raíz).

El nombre de usuario del administrador para el host ESXi es root. De forma predeterminada, la contraseña del administrador no está establecida.

Procedimiento

1 En la consola directa, seleccione **Configurar contraseña**.

2 (opcional) Si ya hay una contraseña configurada, escríbala en la línea **Contraseña antigua** y presione Intro.

3 En la línea **Contraseña nueva**, introduzca una nueva contraseña y presione Intro.

4 Vuelva a introducir la nueva contraseña y presione Intro.

Configuración de arranque del BIOS

Si el servidor tiene varias unidades, es posible que deba configurar las opciones del BIOS.

La configuración de arranque del BIOS determina la manera en que se arranca el servidor. Por lo general, el dispositivo de CD-ROM se muestra primero en la lista.

Nota Si usa ESXi integrado, la configuración de arranque del BIOS determina si el servidor se inicia desde un dispositivo de arranque de ESXi o desde otro dispositivo de arranque. Por lo general, el dispositivo flash USB se muestra primero en la lista de la configuración de arranque del BIOS en la máquina que aloja ESXi.

Es posible cambiar la configuración de arranque configurando el orden de arranque en el BIOS durante el inicio o seleccionado un dispositivo de arranque desde el menú selección de dispositivos de arranque. Cuando se cambia el orden de arranque en el BIOS, la nueva configuración afecta todos los reinicios posteriores. Cuando se selecciona un dispositivo de arranque desde el menú selección de dispositivos de arranque, la selección afecta únicamente el arranque actual.

Algunos servidores no incluyen un menú selección de dispositivos de arranque, en cuyo caso se debe cambiar el orden de arranque en el BIOS incluso para los arranques únicos y, a continuación, se debe volver a cambiar durante un reinicio posterior.

Cómo cambiar la configuración de arranque del BIOS para ESXi

Ajuste la configuración de arranque del BIOS para ESXi si desea que el servidor arranque en ESXi de forma predeterminada.

Las versiones ESXi Instalable y ESXi Integrada, no pueden existir en el mismo host.

Procedimiento

1 Mientras se enciende el host ESXi, presione la tecla necesaria para entrar en la configuración del BIOS del host.

   En función del hardware del servidor, la tecla podría ser una tecla de función o Suprimir. La opción para entrar a la configuración del BIOS podría ser diferente para su servidor.

2 Seleccione la configuración de arranque del BIOS.

Opción	Descripción
Si está utilizando la versión instalable de ESXi	Seleccione el disco en el que instaló el software ESXi y muévalo a la primera posición de la lista. El host arrancará en ESXi.
Si está utilizando la versión integrada de ESXi	Seleccione el dispositivo flash USB y muévalo a la primera posición de la lista. El host arrancará en el modo ESXi.

Configuración de la opción de arranque para medios virtuales

Si usa software de administración remota para configurar ESXi, es posible que deba configurar la opción de arranque para medios virtuales.

Los medios virtuales son una manera de conectar un medio de almacenamiento remoto como CD-ROM, dispositivo de almacenamiento USB, imagen ISO y disquete con un servidor de destino que puede estar en cualquier lado de la red. El servidor de destino tiene acceso al medio remoto, y puede leerlo y escribir en él como si estuviera conectado físicamente al puerto USB del servidor.

Requisitos previos

Las versiones ESXi Instalable y ESXi Integrada, no pueden existir en el mismo host.

Procedimiento

1. Conecte el medio al dispositivo virtual.

   Por ejemplo, si utiliza un servidor Dell, inicie sesión en Dell Remote Access Controller (DRAC) o una interfaz de administración remota similar y seleccione una unidad de disquete o CD-ROM física, o bien proporcione una ruta de acceso a una imagen de disquete o de CD-ROM.

2. Reinicie el servidor.
3. Mientras se enciende el servidor, entre al menú de selección de dispositivos.

   En función del hardware del servidor, la tecla podría ser una tecla de función o Suprimir.

4. Siga las instrucciones para seleccionar el dispositivo virtual.

Resultados

El servidor arranca desde el dispositivo configurado una vez y vuelve al orden de arranque predeterminado en los arranques subsiguientes.

Configuración de las opciones de red

ESXi requiere una dirección IP para la red de administración. Para configurar las opciones de red básicas, utilice vSphere Web Client o la consola directa.

Utilice vSphere Web Client si está conforme con la dirección IP asignada por el servidor DHCP.

Utilice la consola directa para la configuración de red en los casos siguientes:

- Si no está conforme con la dirección IP asignada por el servidor DHCP.
- Si no está autorizado para emplear la dirección IP asignada por el servidor DHCP.
- Si ESXi no tiene una dirección IP. Esta situación podría darse si en la fase de configuración automática no se configuró DHCP correctamente.
- Si se seleccionó el adaptador de red incorrecto durante la fase de configuración automática.

Acceso de red a un host ESXi

El comportamiento predeterminado es configurar la red de administración ESXi con DHCP. Puede anular el comportamiento predeterminado y utilizar una configuración de IP estática para la red de administración después de que se complete la instalación.

Tabla 2-20. Situaciones de configuración de red compatibles con ESXi

Situación	Enfoque
Debe aceptar la configuración de IP ajustada por DHCP.	En la consola directa de ESXi, puede buscar la dirección IP asignada a través de DHCP a la interfaz de administración de ESXi. Puede utilizar esa dirección IP para conectarse al host desde vSphere Web Client y personalizar la configuración, incluido el cambio de la dirección IP de administración.
Una de las siguientes situaciones es real: ■ No tiene un servidor DHCP. ■ El host ESXi no está conectado a un servidor DHCP. ■ El servidor DHCP conectado no funciona de forma correcta.	Durante la fase de configuración automática, el software asigna la dirección IP local de vínculo, que se encuentra en la subred 169.254.x.x/16. La dirección IP asignada aparece en la consola directa. Puede anular la dirección IP local de vínculo mediante la configuración de una dirección IP estática a través de la consola directa.
El host ESXi se conecta a un servidor DHCP en funcionamiento, pero no desea utilizar la dirección IP configurada por DHCP.	Durante la fase de configuración automática, el software asigna una dirección IP configurada por DHCP. Puede realizar la conexión inicial a través de la dirección IP configurada por DHCP. A continuación, puede configurar una dirección IP estática. Si posee un acceso físico al host ESXi, puede anular la dirección IP configurada por DHCP mediante la configuración de una dirección IP estática a través de la consola directa.
Sus directivas de implementación de seguridad no permiten que se enciendan hosts sin configuración en la red.	Siga el procedimiento de configuración en Configurar la red en un host que no se haya adjuntado a la red.

Recomendaciones de seguridad para redes de ESXi

El aislamiento del tráfico de red es fundamental para proteger el entorno de ESXi. Las distintas redes requieren distintos niveles de aislamiento y acceso.

El host ESXi usa varias redes. Emplee las medidas de seguridad que correspondan para cada red y aísle el tráfico de aplicaciones y funciones específicas. Por ejemplo, asegúrese de que el tráfico de VMware vSphere vMotion® no pase por las redes en las que haya máquinas virtuales. El aislamiento impide las intromisiones. Además, por motivos de rendimiento, también se recomienda usar redes separadas.

- Las redes de infraestructura de vSphere se usan para las características como vSphere vMotion, VMware vSphere Fault Tolerance y almacenamiento. Aísle estas redes según sus funciones específicas. Generalmente, no es necesario dirigir estas redes fuera de un rack de servidor físico único.

- Una red de administración aísla los distintos tráficos (tráfico de clientes, de la interfaz de la línea de comandos (CLI) o de la API, y del software de terceros) de otros tráficos. Esta red debe estar accesible únicamente para los administradores de sistemas, redes y seguridad. Use jump box o Virtual Private Network (VPN) para proteger el acceso a la red de administración. Controle estrictamente el acceso dentro de esta red.
- El tráfico de las máquinas virtuales puede transmitirse por medio de una red o de muchas. Puede optimizar el aislamiento de las máquinas virtuales mediante soluciones de firewall virtuales que establezcan reglas de firewall en la controladora de red virtual. Esta configuración se envía junto con una máquina virtual cuando esta se migra de un host a otro dentro del entorno de vSphere.

Selección de los adaptadores de red para la red de administración

El tráfico entre un host ESXi y cualquier software de administración externo se transmite por medio de un adaptador de red Ethernet en el host. Puede usar la consola directa para elegir los adaptadores de red que utiliza la red de administración.

El software de administración externo incluye, entre otros, vCenter Server y el cliente SNMP. A los adaptadores de red en el host se les asigna el nombre vmnic*N*, donde N es un número único que identifica el adaptador de red (por ejemplo, vmnic0, vmnic1 y así sucesivamente).

Durante la fase de configuración automática, el host ESXi selecciona vmnic0 para el tráfico de administración. Puede anular la opción predeterminada seleccionando manualmente el adaptador de red que transmite el tráfico de administración para el host. En algunos casos, se recomienda usar un adaptador de red Gigabit Ethernet para el tráfico de administración. Otra manera de ayudar a garantizar la disponibilidad es seleccionar varios adaptadores de red. El uso de varios adaptadores de red permite las funcionalidades de equilibrio de la carga y conmutación por error.

Procedimiento

1. Desde la consola directa, seleccione **Configurar red de administración** y presione Intro.
2. Seleccione **Adaptadores de red** y presione Intro.
3. Seleccione un adaptador de red y presione Intro.

Resultados

Una vez que la red esté en funcionamiento, puede usar vSphere Web Client para conectar ESXi al host mediante vCenter Server.

Configurar el id. de VLAN

Puede establecer el número de identificador de LAN virtual (VLAN) del host ESXi.

Procedimiento

1. Desde la consola directa, seleccione **Configurar red de administración** y presione Intro.
2. Seleccione **VLAN** y presione Intro.
3. Introduzca un número de identificador de VLAN del 1 al 4094.

Configurar IP para ESXi

De forma predeterminada, DHCP establece la dirección IP, la máscara de subred y la puerta de enlace predeterminada.

Para futuras referencias, anote la dirección IP.

Para que DHCP funcione, el entorno de red debe tener un servidor DHCP. Si DHCP no está disponible, el host asigna la dirección IP local del vínculo, que se encuentra en la subred 169.254.x.x/16. La dirección IP asignada aparece en la consola directa. Si no cuenta con acceso al host a través de monitor físico, puede acceder a la consola directa mediante una aplicación de administración remota. Consulte Usar aplicaciones de administración remota

Si tiene acceso a la consola directa, cuenta con la opción de configurar una dirección de red estática. La máscara de red predeterminada es 255.255.0.0.

Configurar IP desde la consola directa

Si tiene acceso físico al host o acceso remoto a la consola directa, puede usar la consola directa para configurar la dirección IP, la máscara de subred y la puerta de enlace predeterminada.

Procedimiento

1. Seleccione **Configurar red de administración** y presione Intro.
2. Seleccione **Configuración IP** y presione Intro.
3. Seleccione **Establecer dirección IP estática y configuración de red**.
4. Introduzca la dirección IP, la máscara de subred y la puerta de enlace predeterminada y presione Intro.

Configurar IP desde vSphere Web Client

Si no tiene acceso físico al host, puede utilizar vSphere Web Client para establecer la configuración de IP estática.

Procedimiento

1. Inicie sesión en vCenter Server desde vSphere Web Client.
2. Seleccione el host en el inventario.
3. En la pestaña **Configurar**, expanda **Redes**.
4. Seleccione **Adaptadores virtuales**.
5. Seleccione **Red de administración vmk0** y haga clic en el icono de edición.
6. Seleccione **Configuración de IPv4**.
7. Seleccione **Usar configuración de IPv4 estática**.
8. Introduzca o modifique la configuración de la dirección IPv4 estática.

9 (opcional) Configure direcciones IPv6 estáticas.

   a Seleccione **Configuración de IPv6**.

   b Seleccione **Direcciones IPv6 estáticas**.

   c Haga clic en el icono de adición.

   d Escriba la dirección IPv6 y haga clic en **Aceptar**.

10 Haga clic en **Aceptar**.

Configurar DNS para ESXi

Puede seleccionar una configuración de DNS manual o automática del host ESXi.

El valor predeterminado es automático. Para que el DNS funcione, su entorno de red debe tener un servidor DHCP y un servidor DNS.

En entornos de red donde no hay DNS automático o no se desea que haya uno, puede configurar información de DNS estático, incluidos un nombre de host, un servidor de nombres principal, un servidor de nombres secundario y sufijos DNS.

Configurar DNS desde la consola directa

Si tiene acceso físico al host o acceso remoto a la consola directa, puede usar la consola directa para configurar información de DNS.

Procedimiento

1 Seleccione **Configurar red de administración** y presione Intro.

2 Seleccione **Configuración del DNS** y presione Intro.

3 Seleccione **Usar las siguientes direcciones de servidor DNS y nombre de host**.

4 Introduzca el servidor principal, el servidor alternativo (opcional) y el nombre de host.

Configurar sufijos DNS

Si tiene acceso físico al host, puede utilizar la consola directa para configurar la información del DNS. De forma predeterminada, DHCP adquiere los sufijos DNS.

Procedimiento

1 Desde la consola directa, seleccione **Configurar la red de administración**.

2 Seleccione **Personalizar sufijos DNS** y presione Intro.

3 Introduzca los nuevos sufijos DNS.

Configurar la red en un host que no se haya adjuntado a la red

Algunos entornos altamente seguros no permiten que se enciendan hosts no configurados en la red. Puede configurar el host antes de conectarlo a la red.

Requisitos previos

Compruebe que no existan cables de red conectados al host.

Procedimiento

1 Encienda el host.

2 Utilice la interfaz de usuario de la consola directa para configurar la contraseña para la cuenta de administrador (raíz).

3 Utilice la interfaz de usuario de la consola directa para configurar una dirección IP estática.

4 Conecte un cable de red al host.

5 (opcional) Utilice vSphere Web Client para conectarse a un sistema vCenter Server.

6 (opcional) Agregue el host al inventario de vCenter Server.

Probar la red de administración

Puede usar la consola directa para realizar pruebas de conectividad de red sencillas.

La consola directa realiza las siguientes pruebas.

- Hace ping en la puerta de enlace predeterminada
- Hace ping en el servidor de nombre del DNS principal
- Hace ping en el servidor de nombre del DNS secundario
- Resuelve el nombre de host configurado

Procedimiento

1 Desde la consola directa, seleccione **Probar red de administración** y presione Intro.

2 Presione Intro para comenzar la prueba.

Reiniciar los agentes de administración

Los agentes de administración sincronizan los componentes de VMware y permiten acceder al host ESXi mediante vSphere Web Client y vCenter Server. Se instalan con el software vSphere. Es posible que necesite reiniciar los agentes de administración si se interrumpe el acceso remoto.

Al reiniciar los agentes de administración, se reinician todos los agentes de administración y los servicios que están instalados y se ejecutan en `/etc/init.d` en el host ESXi. Generalmente, estos agentes incluyen hostd, ntpd, sfcbd, slpd, wsman y vobd. El software también reinicia Fault Domain Manager (FDM) si está instalado.

Los usuarios que accedan a este host a través de vSphere Web Client y vCenter Server perderán la conectividad cuando reinicie los agentes de administración.

Procedimiento

1 Desde la consola directa, seleccione **Opciones de solución de problemas** y presione Intro.

2 Seleccione **Reiniciar agentes de administración** y presione Intro.

3 Presione F11 para confirmar el reinicio.

Resultados

El host ESXi reiniciará los servicios y los agentes de administración.

Reiniciar la red de administración

Puede que sea necesario reiniciar la interfaz de red de administración para restaurar la red o renovar una concesión de DHCP.

Si se reinicia la red de administración, se produce una breve interrupción de red que puede afectar temporalmente a las máquinas virtuales en ejecución.

Si una concesión de DHCP renovada provoca una nueva identidad de red (dirección IP o nombre de host), se desconecta el software de administración remota.

Procedimiento

1 Desde la consola directa, seleccione **Reiniciar red de administración** y presione Intro.

2 Presione F11 para confirmar el reinicio.

Prueba de la conectividad con los dispositivos y las redes

Puede utilizar la consola directa para realizar algunas pruebas simples de conectividad de red. Además de la red de administración, se pueden especificar otros dispositivos y otras redes.

Procedimiento

1 Desde la consola directa, seleccione **Probar red de administración** y presione Intro.

2 Escriba las direcciones a las que desee emitir un ping u otro nombre de host DNS que desee resolver.

3 Presione Intro para comenzar la prueba.

Restauración del conmutador estándar

vSphere Distributed Switch funciona como un único conmutador virtual en todos los hosts asociados. Las máquinas virtuales pueden mantener una configuración de red coherente cuando se migran a varios hosts. Si migra un conmutador estándar existente o un adaptador virtual a Distributed Switch, y este deja de ser necesario o deja de funcionar, puede restaurar el conmutador estándar para asegurarse de que el host siga estando accesible.

Cuando restaura el conmutador estándar, se crea un nuevo adaptador virtual y el vínculo superior de red de administración conectado actualmente a Distributed Switch se migra al nuevo conmutador virtual.

Es posible que necesite restaurar el conmutador estándar por las siguientes razones:

- Distributed Switch no se necesita o no funciona.

- Es necesario reparar Distributed Switch para restaurar la conectividad con vCenter Server y los hosts deben permanecer accesibles.
- No es deseable que vCenter Server administre el host. Cuando el host no está conectado a vCenter Server, la mayoría de las características de Distributed Switch no están disponibles para el host.

Requisitos previos

Compruebe que la red de administración esté conectada a un conmutador distribuido.

Procedimiento

1 En la consola directa, seleccione **Restaurar conmutador estándar** y presione Intro.

  Si el host se encuentra en un conmutador estándar, la opción aparece atenuada y no puede seleccionarla.

2 Presione F11 para confirmar.

Comportamiento de almacenamiento

Al iniciar ESXi, el host entra en una fase de autoconfiguración durante la que se configuran los dispositivos de almacenamiento del sistema con los valores predeterminados.

Cuando reinicie el host ESXi después de instalar la imagen de ESXi, el host configura los dispositivos de almacenamiento del sistema con la configuración predeterminada. De forma predeterminada, todos los discos internos vacíos visibles se formatean con VMFS a fin de que sea posible almacenar máquinas virtuales en los discos. En ESXi Embedded, todos los discos internos vacíos visibles con VMFS también se formatean de forma predeterminada.

Precaución ESXi sobrescribe cualquier disco que parezca estar vacío. Los discos se consideran vacíos si no poseen una tabla de particiones o particiones válidas. Si usa software que utiliza dichos discos, en particular si está utilizando un administrador de volúmenes lógicos (LVM) en lugar de o además de esquemas tradicionales de particionamiento, ESXi podría causar un reformateo del LVM local. Realice una copia de seguridad de los datos del sistema antes de habilitar ESXi por primera vez.

En el disco duro o dispositivo USB desde el que arranca el host ESXi, el software de formateo de discos conserva las particiones de diagnóstico existentes que el proveedor de hardware crea. En el espacio restante, el software crea las particiones descritas en Tabla 2-21. Particiones creadas por ESXi en la unidad del host.

Tabla 2-21. Particiones creadas por ESXi en la unidad del host

Versión de ESXi	Particiones creadas
ESXi Installable	Para instalaciones desde cero, se crean varias particiones nuevas para los bancos de arranque, la partición de trabajo y el bloqueador. La instalaciones desde cero de ESXi utilizan las tablas de particiones GUID (GPT) en lugar del particionamiento basado en MSDOS. La tabla de particiones en sí se establece como parte de la imagen binaria y se escribe en el disco en el mismo momento que se instala el sistema. El instalador de ESXi deja las particiones de trabajo y de VMFS vacías, y ESXi las crea cuando el host se reinicia por primera vez después de la instalación o actualización. Solo se crea una partición de trabajo VFAT de 4 GB para el intercambio de sistema. Consulte Acerca de la partición desde cero. La partición de trabajo VFAT se crea solo en el disco desde el que se arranca el host ESXi. **Nota** Para crear el volumen VMFS y una partición de trabajo con la instalación, el instalador de ESXi requiere un mínimo de 5,2 GB de espacio libre en el disco de instalación. El instalador afecta solamente al disco de instalación. El instalador no afecta a otros discos del servidor. Cuando se realiza la instalación en un disco, el instalador sobrescribe el disco completo. Cuando el instalador configura automáticamente el almacenamiento, no sobrescribe las particiones del proveedor de hardware. Durante la instalación de ESXi, el instalador crea una partición de diagnóstico de 110 MB para los volcados de memoria.
ESXi Embedded	Una partición de diagnóstico de 110 MB para los volcados de memoria, si la partición no está presente en otro disco. Las particiones de trabajo y diagnóstico VFAT se crean solo en el disco desde el que se arranca el host ESXi. En otros discos, el software crea una partición VMFS5 por disco vacío, utilizando todo el disco. Solo se formatean los discos vacíos.
ESXi Installable y ESXi Embedded	Una partición VMFS5 en el espacio libre restante.

Es posible que desee anular este comportamiento predeterminado si, por ejemplo, utiliza dispositivos de almacenamiento compartido en lugar de almacenamiento local. A fin de evitar un formateo automático de discos, desconecte los dispositivos de almacenamiento local del host en las siguientes circunstancias:

- Antes de ejecutar el host por primera vez.
- Antes de ejecutar el host después de restablecerlo a los valores predeterminados de configuración.

Para anular el formateo VMFS, si ya se realizó el formateo automático de discos, puede eliminar el almacén de datos. Consulte la documentación de *Administrar vCenter Server y hosts*.

Acerca de la partición desde cero

Para nuevas instalaciones de ESXi, durante la fase de configuración automática se crea una partición VFAT de 4 GB desde cero si la partición no esté presente en otro disco.

Nota La creación de particiones de los hosts que se actualizan a ESXi 5.x desde versiones de ESXi anteriores a la 5.0 se diferencia en gran medida de la creación de particiones para nuevas instalaciones de ESXi 5.x. Consulte la documentación de *Actualizar vSphere*.

Cuando ESXi arranca, el sistema intenta buscar una partición adecuada en un disco local para crear una partición desde cero.

No se requiere la partición desde cero. Se usa para almacenar la salida de vm-support que se necesita cuando se crea un paquete compatible. Si no hay una partición desde cero, la salida de vm-support se almacena en un ramdisk. En situaciones con poca memoria, sería conveniente crear una partición desde cero si no hay una presente.

Para la versión instalable de ESXi, la partición se crea durante la instalación y se selecciona. VMware recomienda que no modifique la partición.

Nota Para crear el volumen y la partición desde cero de VMFS, el instalador de ESXi necesita un mínimo de 5,2 GB de espacio disponible en el disco de instalación.

Para ESXi Embedded, si no se encuentra una partición pero hay un disco local vacío, el sistema lo formatea y crea una partición desde cero. Si no se crea una partición desde cero, se puede configurar una, pero no es necesario que esta exista. También puede anular la configuración predeterminada. Sería conveniente crear la partición desde cero en un directorio remoto montado en NFS.

Nota El instalador puede crear varias particiones de VFAT. La designación de VFAT no siempre indica que la partición sea desde cero. En ocasiones, una partición de VFAT simplemente puede permanecer inactiva.

Establecer la partición desde cero de vSphere Web Client

Si no hay ninguna partición desde cero configurada, es posible que quiera configurar una, especialmente si le preocupa la memoria insuficiente. Si no hay una partición desde cero, el resultado de vm-support se almacena en un disco RAM.

Requisitos previos

El directorio que se usará para la partición temporal debe existir en el host.

Procedimiento

1 Desde vSphere Web Client, conéctese a vCenter Server.

2 Seleccione el host en el inventario.

3 Haga clic en la pestaña **Administrar**.

4 Seleccione **Configuración**.

5 Seleccione **Configuración avanzada del sistema**.

   El parámetro **ScratchConfig.CurrentScratchLocation** muestra la ubicación actual de la partición desde cero.

6 En el cuadro de texto **ScratchConfig.ConfiguredScratchLocation**, introduzca una ruta de acceso de directorio que sea exclusiva para este host.

   Por ejemplo, **`/vmfs/volumes/`*`DatastoreUUID`*`/`*`DatastoreFolder`***.

7 Reinicie el host para que se apliquen los cambios.

Configurar el registro del sistema

Los hosts ESXi ejecutan el servicio syslog (`vmsyslogd`), que escribe mensajes de VMkernel y otros componentes del sistema en archivos de registro.

Puede configurar la cantidad y la ubicación del registro. También puede crear y aplicar filtros de registro para modificar la directiva de registro de un host ESXi.

Configurar Syslog en hosts ESXi

Puede utilizar vSphere Web Client o el comando `esxcli system syslog` de vCLI para configurar el servicio de Syslog.

Para obtener información sobre la utilización del comando `esxcli system syslog` y otros comandos de vCLI, consulte *Introducción a vSphere Command-Line Interface*.

Procedimiento

1 En el inventario de vSphere Web Client, seleccione el host.

2 Haga clic en **Configurar**.

3 En Sistema, haga clic en **Configuración avanzada del sistema**.

4 Filtre por **`syslog`**.

5 Para configurar el registro de manera global, seleccione la configuración que desea cambiar y haga clic en **Editar**.

Opción	Descripción
Syslog.global.defaultRotate	Cantidad máxima de archivos que desea guardar. Puede configurar este número en forma global y para subregistradores individuales.
Syslog.global.defaultSize	Tamaño predeterminado del registro, en KB, antes de que el sistema rote los registros. Puede configurar este número en forma global y para subregistradores individuales.

Opción	Descripción
Syslog.global.LogDir	El directorio en el que se almacenan los registros. El directorio puede estar ubicado en volúmenes de NFS o VMFS montados. Solo el directorio `/scratch` del sistema de archivos local se mantiene en todos los reinicios. Especifique el directorio como [*datastorename*] *path_to_file*, donde la ruta de acceso es relativa a la raíz del volumen que respalda el almacén de datos. Por ejemplo, la ruta de acceso `[storage1] /systemlogs` se asigna a la ruta de acceso `/vmfs/volumes/storage1/systemlogs`.
Syslog.global.logDirUnique	Al seleccionar esta opción, se crea un subdirectorio con el nombre del host ESXi del directorio especificado por **Syslog.global.LogDir**. Un directorio único es útil si varios hosts ESXi utilizan el mismo directorio NFS.
Syslog.global.LogHost	El host remoto al que se reenvían los mensajes de syslog y el puerto en el que el host remoto recibe mensajes de syslog. Puede incluir el protocolo y el puerto; por ejemplo, `ssl://hostName1:1514`. Se admiten UDP (predeterminado), TCP y SSL. El host remoto debe tener syslog instalado y configurado correctamente para recibir los mensajes de syslog reenviados. Consulte la documentación del servicio de Syslog instalado en el host remoto para obtener información sobre la configuración.

6 (Opcional) Para sobrescribir los valores predeterminados del tamaño de registro y la rotación de registros de cualquier registro.

   a Haga clic en el nombre del registro que desea personalizar.

   b Haga clic en **Editar** y escriba el número de rotaciones y el tamaño de registro que desea.

7 Haga clic en **Aceptar**.

Resultados

Los cambios en las opciones de syslog se aplican de inmediato.

Configurar el filtrado de registros en hosts ESXi

Las capacidades de filtrado de registros permiten modificar la directiva de registro del servicio de Syslog que se ejecuta en un host ESXi. Puede crear filtros de registros para reducir la cantidad de entradas repetidas en los registros de ESXi y agregar a la lista de no permitidos eventos de registros específicos en su totalidad.

Los filtros de registros afectan a todos los eventos de registros que el daemon vmsyslogd del host ESXi procesa, ya sea que se registren en un directorio de registro o en un servidor remoto de Syslog.

Al crear un filtro de registro, se establece una cantidad máxima de entradas de registro para los mensajes de registro. Los mensajes de registros son generados por uno o más componentes del sistema especificado y coinciden con una frase especificada. Debe habilitar la capacidad de filtrado de registros y volver a cargar el daemon de Syslog para activar los filtros de registros en el host ESXi.

Importante Al establecer un límite para la cantidad de información de registro, se restringe la capacidad para solucionar correctamente los posibles errores del sistema. Si ocurre una rotación de registros después de que se alcance la cantidad máxima de entradas de registro, es posible que pierda todas las instancias de un mensaje filtrado.

Procedimiento

1 Inicie sesión en ESXi Shell como raíz.

2 En el archivo `/etc/vmware/logfilters`, agregue la siguiente entrada para crear un filtro de registro.

```
numLogs | ident | logRegexp
```

donde:

- *numLogs* establece la cantidad máxima de entradas de registro para los mensajes de registro especificados. Una vez alcanzado este número, se filtran y se omiten los mensajes de registro especificados. Utilice **0** para filtrar y omitir todos los mensajes de registro especificados.
- *ident* especifica uno o más componentes del sistema para aplicar el filtro a los mensajes de registro que generan estos componentes. Para obtener información sobre los componentes del sistema que generan los mensajes de registro, consulte los valores de los parámetros de `idents` en los archivos de configuración de syslog. Los archivos se encuentran en el directorio `/etc/vmsyslog.conf.d`. Utilice una lista separada por comas para aplicar un filtro a varios componentes del sistema. Utilice ***** para aplicar un filtro a todos los componentes del sistema.
- *logRegexp* especifica una frase que distingue mayúsculas de minúsculas con la sintaxis de la expresión regular Python para filtrar los mensajes de registro según su contenido.

Por ejemplo, para establecer un límite máximo de dos entradas de registro desde el componente hostd para mensajes que se asemejen a la frase `SOCKET connect failed, error 2: No such file or directory` con cualquier número de error, agregue la siguiente entrada:

```
2 | hostd | SOCKET connect failed, error .*: No such file or directory
```

Nota Una línea que comienza con `#` indica un comentario y se omite el resto de la línea.

3 En el archivo `/etc/vmsyslog.conf`, agregue la siguiente entrada para habilitar la capacidad de filtrado de registros.

```
enable_logfilters = true
```

4 Ejecute el comando `esxcli system syslog reload` para volver a cargar el daemon Syslog y aplicar los cambios de configuración.

Configurar el nivel de aceptación del perfil de imagen de host

El nivel de aceptación del perfil de imagen del host determina qué paquetes de instalación de vSphere (VIB) se aceptan para la instalación.

Las firmas de VIB se comprueban y se aceptan para la instalación según una combinación del nivel de aceptación de VIB y nivel de aceptación del perfil de imagen del host. Los VIB se etiquetan con un nivel de aceptación que depende del estado de la firma.

Consulte Niveles de aceptación.

Requisitos previos

Privilegios requeridos: **Host.Configuration.Security Profile** and **Host.Configuration.Firewall**

Procedimiento

1 Desde vSphere Web Client, conéctese a vCenter Server.

2 Seleccione el host en el inventario.

3 Haga clic en la pestaña **Administrar**.

4 Haga clic en **Configuración**.

5 En Sistema, seleccione **Perfil de seguridad**.

6 Desplácese hacia abajo hasta Nivel de aceptación del perfil de imagen del host y haga clic en **Editar**.

7 Seleccione el nivel de aceptación y haga clic en **Aceptar**.

Tabla 2-22. Niveles de aceptación del perfil de imagen del host

Nivel de aceptación del perfil de imagen del host	Niveles aceptados de los VIB
Certificado por VMware	Certificado por VMware
Aceptado por VMware	Certificado por VMware, Aceptado por VMware
Creado por los partners	Certificado por VMware, Aceptado por VMware, Creado por los partners
Creado por la comunidad	Certificado por VMware, Aceptado por VMware, Creado por los partners, Creado por la comunidad

Quitar todos los paquetes personalizados en ESXi

Después de agregar paquetes personalizados, puede que se decida quitarlos.

Requisitos previos

Antes de quitar paquetes personalizados, apague o migre las máquinas virtuales en ejecución fuera del host ESXi.

Procedimiento

1 Reinicie el host ESXi.

2 En la consola directa, seleccione **Quitar extensiones personalizadas** y presione F11 para confirmar.

3 Reinicie el host.

Resultados

Se quitan todos los paquetes personalizados.

Deshabilitación de la compatibilidad con caracteres no ASCII en los nombres de directorios y archivos de máquinas virtuales

De forma predeterminada, ESXi admite el uso de caracteres no ASCII para los nombres de directorios y archivos de máquinas virtuales. Para deshabilitar esto, modifique el archivo `/etc/vmware/hostd/config.xml`.

Una vez que deshabilite esta compatibilidad, podrá seguir introduciendo caracteres no ASCII en los nombres de las máquinas virtuales. Las interfaces de usuario de vSphere muestran los nombres de las máquinas virtuales en caracteres no ASCII, pero ESXi convierte los nombres del archivo en cuestión y los nombres de directorios en cadenas ASCII.

Procedimiento

1 Mediante un editor de texto, abra el archivo `/etc/vmware/hostd/config.xml` para el host ESXi.

2 En la etiqueta `<config></config>`, agregue el código siguiente.

```
<g11nSupport>false</g11nSupport>
```

3 Guarde y cierre el archivo.

4 Reinicie el host.

Restablecer la configuración del sistema

Si tiene problemas para determinar el origen de un problema con su host ESXi, puede restablecer la configuración del sistema.

Los cambios en la configuración del sistema pueden estar relacionados con diferentes problemas, incluidos los problemas de conectividad con la red y dispositivos. Restablecer la configuración del sistema podría resolver estos problemas. Si restablecer la configuración del sistema no resuelve el problema, puede descartar los cambios en la configuración realizados desde la configuración inicial como el origen del problema.

Cuando restablezca la configuración, el software anula todos los cambios en la configuración, elimina la contraseña de la cuenta de administrador (raíz) y reinicia el host. También podrían eliminarse los cambios en la configuración realizados por el proveedor del hardware, como la configuración de direcciones IP y la configuración de licencias.

El restablecimiento de la configuración no elimina las máquinas virtuales del host ESXi. Después de restablecer los valores predeterminados de configuración, las máquinas virtuales no aparecen visibles, pero puede volver a lograr que estén visibles reconfigurando el almacenamiento y volviendo a registrar las máquinas virtuales.

Precaución Cuando restablezca los valores predeterminados de configuración, los usuarios que están accediendo al host pierden conectividad.

Requisitos previos

Antes de restablecer la configuración, realice una copia de seguridad de su configuración de ESXi en caso de que desee restaurar su configuración.

Procedimiento

1 Realice una copia de seguridad de la configuración utilizando el comando `vicfg-cfgbackup` de vSphere CLI.

2 Desde la consola directa, seleccione **Restablecer la configuración del sistema** y presione Intro.

3 Presione F11 para confirmar.

Resultados

El sistema se reiniciará después de que la configuración se restablezca a los valores predeterminados.

Después de instalar y configurar ESXi

Una vez que ESXi está instalado y configurado, puede administrar el host mediante vSphere Web Client y vCenter Server, aplicar una licencia al host y crear una copia de seguridad de la configuración de ESXi.

También puede usar VMware Host Client para conectarse directamente al host ESXi y administrarlo. Para obtener información sobre cómo instalar y utilizar VMware Host Client, consulte *Administrar un host único de vSphere*.

Administrar el host ESXi

VMware Host Client ofrece la forma más sencilla de administrar el host ESXi y controlar las máquinas virtuales.

También puede utilizar vSphere Web Client para conectarse y administrar vCenter Server a través de un explorador web. vSphere Web Client se instala junto con vCenter Server y vCenter Server Appliance, y puede utilizarlo para administrar sus hosts ESXi.

Licencias de hosts ESXi

Después de instalar ESXi, el software ofrece un período de evaluación de 60 días durante el cual se puede explorar el conjunto completo de funciones de vSphere que se obtienen con una licencia de vSphere Enterprise Plus. Debe asignar al host una licencia adecuada antes de que caduque el período de evaluación.

Los hosts ESXi incluyen licencias de vSphere que proporcionan capacidad por CPU. Para proporcionar las licencias correctas a los hosts, debe asignarles una licencia de vSphere que cuente con capacidad de CPU suficiente para abarcar todos los CPU de los hosts. La licencia debe admitir todas las funciones que utilizan los hosts. Por ejemplo, si los hosts están conectados a vSphere Distributed Switch, debe asignarles una licencia que incluya la característica vSphere Distributed Switch.

Puede emplear uno de los métodos siguientes para asignar licencias a los hosts ESXi:

- Asignar licencias a varios hosts a la vez mediante la función de administración de licencias de vSphere Web Client. Los hosts deben estar conectados a un sistema vCenter Server. Para obtener más información, consulte *Administrar vCenter Server y hosts*.
- Configurar licencias masivas mediante los comandos de PowerCLI. Las licencias masivas funcionan para todos los hosts ESXi, pero son especialmente útiles para los hosts aprovisionados con Auto Deploy. Consulte Configurar licencias masivas
- Otorgue licencias a hosts ESXi individuales mediante el uso de una conexión directa con VMware Host Client. Para obtener información sobre cómo asignar una clave de licencia para un host ESXi, consulte *Administrar un host único de vSphere*.

Acerca de los modos de evaluación y con licencia de ESXi

Puede utilizar el modo de evaluación para explorar el conjunto completo de funciones para los hosts ESXi. El modo de evaluación proporciona un conjunto de funciones equivalente a una licencia de vSphere Enterprise Plus. Antes de que finalice el modo de evaluación, debe asignar a sus hosts una licencia que admita todas las funciones en uso.

Por ejemplo, en el modo de evaluación, puede utilizar la tecnología vSphere vMotion, la función vSphere HA, la característica vSphere DRS y otras características. Si desea continuar utilizando estas funciones, debe asignar una licencia que las admita.

La versión de los hosts ESXi Installable se instala siempre en el modo de evaluación. ESXi Embedded se ofrece preinstalado en el dispositivo de almacenamiento interno por parte de cada proveedor de hardware. Podría estar en el modo de evaluación o con licencia previa.

El período de evaluación es de 60 días y comienza cuando se enciende el host ESXi. En cualquier momento durante el período de evaluación de 60 días, se puede realizar la conversión de un modo con licencia a un modo de evaluación. El tiempo disponible en el modo de evaluación se resta del tiempo ya consumido.

Por ejemplo, supongamos que se utiliza un host ESXi en el modo de evaluación durante 20 días y, a continuación, se asigna una clave de licencia de vSphere Standard Edition al host. Si se vuelve a establecer el host en el modo de evaluación, se podrá explorar el conjunto completo de funciones para el host durante el período de evaluación restante de 40 días.

Para obtener información sobre la administración de licencias para los hosts ESXi, consulte la documentación *Administrar vCenter Server y hosts*.

Registro de la clave de licencia de un host ESXi

Si no es posible acceder a un host o arrancarlo, deberá tener un registro de su clave de licencia. Puede escribir la clave de licencia y pegarla con cinta en el servidor o colocar la clave de licencia en una ubicación segura. Puede acceder a la clave de licencia desde la interfaz de usuario de la consola directa o vSphere Web Client.

Ver las claves de licencia de los hosts ESXi desde vSphere Web Client

Puede ver las claves de licencia de los hosts que están conectados a un sistema vCenter Server a través de vSphere Web Client.

Procedimiento

1 En vSphere Web Client, seleccione **Administración**.
2 En Licencias, seleccione **Licencias**.
3 En la pestaña **Activos**, seleccione **Hosts**.
4 En la columna Licencia, haga clic en una licencia.

Resultados

Verá información sobre la licencia, como su uso y la clave de licencia.

Acceder a la clave de licencia de ESXi desde la consola directa

Si tiene acceso físico al host o acceso remoto a la consola directa, puede utilizar la consola directa para acceder a la clave de licencia de ESXi.

Procedimiento

- En la consola directa, seleccione **Ver información de soporte**.

  La clave de licencia aparece con el formato XXXXX-XXXXX-XXXXX-XXXXX-XXXXX, etiquetada como Número de serie de la licencia.

  Nota También aparece el número de serie del equipo físico, etiquetado como Número de serie. No confunda la clave de licencia con el número de serie del equipo físico.

Ver registros del sistema

Los registros del sistema proporcionan información detallada sobre los eventos operativos del sistema.

Procedimiento

1 En la consola directa, seleccione **Ver registros del sistema**.

2 Presione la tecla numérica que corresponda para ver un registro.

   Si agrega el host a vCenter Server, aparecen los registros de vCenter Server Agent (vpxa).

3 Presione Intro o la barra espaciadora para desplazarse por los mensajes.

4 Realice una búsqueda de expresiones regulares.

   a Presione la tecla de barra diagonal (/).

   b Escriba el texto que desea buscar.

   c Presione Intro.

   El texto que se encontró aparece resaltado en la pantalla.

5 Presione q para volver a la consola directa.

Pasos siguientes

Consulte también Configurar Syslog en hosts ESXi.

Implementar vCenter Server Appliance y el dispositivo de Platform Services Controller

3

Es posible implementar vCenter Server Appliance con una instancia integrada o externa de Platform Services Controller para administrar el entorno de vSphere. Es posible implementar un dispositivo de Platform Services Controller, así como registrar las implementaciones externas y las instalaciones en Windows de vCenter Server Appliance con este dispositivo de Platform Services Controller.

Es posible implementar vCenter Server Appliance o el dispositivo de Platform Services Controller en un host ESXi 5.5 o posterior, o en un host ESXi o un clúster de DRS desde el inventario de una instancia de vCenter Server 5.5 o posterior.

Para obtener información sobre el software que se incluye en vCenter Server Appliance 6.5, consulte Descripción general de vCenter Server Appliance.

Para obtener información sobre los requisitos de software y hardware para implementar vCenter Server Appliance y el dispositivo de Platform Services Controller, consulte Requisitos de sistema para el dispositivo vCenter Server Appliance y Platform Services Controller.

Una alternativa es usar los archivos ejecutables para implementaciones de GUI y CLI que se incluyen en el instalador de vCenter Server Appliance.

- La implementación de GUI es un proceso de dos etapas. En la primera etapa, un asistente de implementación implementa el archivo OVA para el dispositivo en el host ESXi o la instancia de vCenter Server de destino. Una vez completada la implementación de OVA, el usuario es redirigido a la segunda etapa del proceso en la que se instalan y se inician los servicios del dispositivo recién implementado.
- El método de implementación de CLI implica ejecutar un comando de CLI en un archivo JSON preparado previamente. El instalador de CLI analiza los parámetros de configuración y los valores indicados en el archivo JSON, y genera un comando de OVF Tool para implementar y configurar automáticamente el dispositivo.

Importante Para usar topologías con instancias externas de Platform Services Controller, es necesario implementar las instancias de replicación de Platform Services Controller en secuencia. Después de implementar correctamente todas las instancias de Platform Services Controller en el dominio, se pueden realizar implementaciones simultáneas de varios dispositivos de vCenter Server que apuntan a una instancia externa común de Platform Services Controller.

---

vCenter Server Appliance y el dispositivo de Platform Services Controller contienen los siguientes nombres de usuario predeterminados:

Nombre de usuario	Descripción
root	Utilice este nombre de usuario para iniciar sesión en el sistema operativo de un dispositivo y la interfaz de administración de dispositivos. La contraseña se establece durante la implementación del dispositivo virtual.
administrator@*su_nombre_de_dominio*	Utilice este nombre de usuario para iniciar sesión en vCenter Single Sign-On. La contraseña se establece durante la creación del dominio de vCenter Single Sign-On. El dominio de vCenter Single Sign-On se crea durante la implementación de una instancia de vCenter Server Appliance con un dispositivo de Platform Services Controller integrado o la primera instancia de Platform Services Controller en un dominio de vCenter Single Sign-On nuevo. Después de que se cree un dominio de vCenter Single Sign-On, solo el usuario administrator@*su_nombre_de_dominio* contará con los privilegios necesarios para iniciar sesión en vCenter Single Sign-On y vCenter Server. El usuario administrator@*su_nombre_de_dominio* puede proceder de la siguiente manera: ■ Agregar un origen de identidad en el cual los usuarios y grupos tienen definido vCenter Single Sign-On. ■ Otorgar permisos a los usuarios y grupos. Para obtener información sobre cómo agregar orígenes de identidad y conceder permisos a usuarios y grupos, consulte *Administrar Platform Services Controller*.

Para obtener información sobre la actualización y la revisión de vCenter Server Appliance y el dispositivo de Platform Services Controller, consulte *Actualizar vSphere*.

Para obtener información sobre la configuración de vCenter Server Appliance y el dispositivo de Platform Services Controller, consulte *Configuración de vCenter Server Appliance*.

Si desea configurar vCenter Server Appliance para usar una versión de dirección IPv6, utilice el nombre de dominio completo (FQDN) o el nombre de host del dispositivo. Para configurar una dirección IPv4, la práctica recomendada es usar el FQDN o nombre de host del dispositivo, ya que la dirección IP puede cambiar si se asigna mediante DHCP.

Este capítulo incluye los siguientes temas:

- Requisitos de sistema para el dispositivo vCenter Server Appliance y Platform Services Controller
- Prepararse para implementar vCenter Server Appliance y el dispositivo de Platform Services Controller
- Requisitos previos para implementar vCenter Server Appliance o el dispositivo de Platform Services Controller
- Implementación de la GUI de vCenter Server Appliance y del dispositivo de Platform Services Controller
- Implementación de CLI en vCenter Server Appliance y en el dispositivo de Platform Services Controller

Requisitos de sistema para el dispositivo vCenter Server Appliance y Platform Services Controller

Puede implementar la instancia de vCenter Server Appliance o el dispositivo de Platform Services Controller en un host ESXi 5.5 o una versión posterior, o en una instancia de vCenter Server 5.5 o una versión posterior. El sistema también debe cumplir con los requisitos específicos de software y hardware.

Al usar nombres de dominios completos, asegúrese de que el equipo cliente que use para implementar el dispositivo y la red en la que implementa el dispositivo utilicen el mismo servidor DNS.

Antes de implementar el dispositivo , sincronice los relojes del servidor de destino y todas las instancias de vCenter Server y Platform Services Controller de la red de vSphere. Los relojes sin sincronizar pueden ocasionar problemas de autenticación y pueden producir un error en la instalación o impedir que se inicien los servicios del dispositivo. Consulte Sincronizar los relojes en la red de vSphere.

Requisitos de hardware para el dispositivo de vCenter Server Appliance y Platform Services Controller

Cuando implemente vCenter Server Appliance, puede seleccionar implementar un dispositivo que sea adecuado para el tamaño del entorno de vSphere. La opción que seleccione determina la cantidad de CPU y la cantidad de memoria para el dispositivo. El tamaño del dispositivo de Platform Services Controller es el mismo para todos los tamaños de entornos.

Requisitos de hardware para vCenter Server Appliance

Los requisitos de hardware para vCenter Server Appliance dependen del tamaño del inventario de vSphere.

Tabla 3-1. Requisitos de hardware para vCenter Server Appliance con una instancia integrad o externa de Platform Services Controller

	Cantidad de vCPU	Memoria
Entorno muy pequeño (hasta 10 hosts o 100 máquinas virtuales)	2	10 GB
Entorno pequeño (hasta 100 hosts o 1.000 máquinas virtuales)	4	16 GB
Entorno mediano (hasta 400 hosts o 4.000 máquinas virtuales)	8	24 GB

Tabla 3-1. Requisitos de hardware para vCenter Server Appliance con una instancia integrad o externa de Platform Services Controller (continuación)

	Cantidad de vCPU	Memoria
Entorno grande (hasta 1.000 hosts o 10.000 máquinas virtuales)	16	32 GB
Entorno extragrande (hasta 2.000 hosts o 35.000 máquinas virtuales)	24	48 GB

Nota Si desea agregar un host ESXi con más de 512 LUN y 2.048 rutas de acceso al inventario de vCenter Server Appliance, debe implementar vCenter Server Appliance para un entorno grande o extragrande.

Requisitos de hardware para el dispositivo de Platform Services Controller

Los requisitos de hardware para un dispositivo de Platform Services Controller son 2 vCPU y 4 GB de memoria.

Requisitos de almacenamiento para el dispositivo de vCenter Server Appliance y Platform Services Controller

Al implementar vCenter Server Appliance o el dispositivo de Platform Services Controller, el host ESXi o el clúster de DRS en el que se implementa el dispositivo debe cumplir con los requisitos mínimos de almacenamiento. El almacenamiento necesario depende no solo del tamaño del entorno de vSphere y del tamaño del almacenamiento, sino también del modo de aprovisionamiento del disco.

Requisitos de almacenamiento para vCenter Server Appliance

Los requisitos de almacenamiento son diferentes para cada tamaño de entorno de vSphere y dependen de los requisitos de tamaño de la base de datos.

Tabla 3-2. Requisitos de almacenamiento para vCenter Server Appliance con una instancia integrada o externa de Platform Services Controller

	Tamaño de almacenamiento predeterminado	Tamaño de almacenamiento grande	Tamaño de almacenamiento extragrande
Entorno muy pequeño (hasta 10 hosts o 100 máquinas virtuales)	250 GB	775 GB	1.650 GB
Entorno pequeño (hasta 100 hosts o 1.000 máquinas virtuales)	290 GB	820 GB	1.700 GB
Entorno mediano (hasta 400 hosts o 4.000 máquinas virtuales)	425 GB	925 GB	1.805 GB

Tabla 3-2. Requisitos de almacenamiento para vCenter Server Appliance con una instancia integrada o externa de Platform Services Controller (continuación)

	Tamaño de almacenamiento predeterminado	Tamaño de almacenamiento grande	Tamaño de almacenamiento extragrande
Entorno grande (hasta 1.000 hosts o 10.000 máquinas virtuales)	640 GB	990 GB	1.870 GB
Entorno extragrande (hasta 2.000 hosts o 35.000 máquinas virtuales)	980 GB	1.030 GB	1.910 GB

Nota Los requisitos de almacenamiento incluyen los requisitos de la instancia de VMware Update Manager que se ejecuta como servicio en el vCenter Server Appliance.

Requisitos de almacenamiento para el dispositivo de Platform Services Controller

El requisito de almacenamiento para un dispositivo de Platform Services Controller es de 60 GB.

Requisitos de software para el dispositivo de vCenter Server Appliance y Platform Services Controller

El dispositivo de vCenter Server Appliance y Platform Services Controller de VMware se pueden implementar en hosts ESXi 5.5 o posteriores o en instancias de vCenter Server 5.5 o posteriores.

Se puede implementar el dispositivo de vCenter Server Appliance o Platform Services Controller por medio de la GUI o del instalador de CLI. Se ejecuta el instalador de un equipo cliente en red que se utiliza para conectarse al servidor de destino e implementar el dispositivo en el servidor. Puede conectarse directamente a un host ESXi 5.5.x o 6.x para implementar el dispositivo allí. Puede conectarse a una instancia de vCenter Server 5.5.x o 6.x para implementar el dispositivo en un host ESXi o clúster de DRS que reside en el inventario de vCenter Server.

Para obtener información sobre los requisitos del equipo cliente en red, consulte Requisitos del sistema para el instalador de vCenter Server Appliance.

Puertos necesarios para vCenter Server y Platform Services Controller

El sistema vCenter Server, tanto en Windows como en el dispositivo, debe poder enviar datos a cada host administrado y recibir datos de los servicios de vSphere Web Client y Platform Services Controller. Para permitir las actividades de migración y aprovisionamiento entre los hosts administrados, los hosts de origen y de destino deben poder recibir datos de cada uno.

Se puede acceder a vCenter Server a través de los puertos TCP y UDP predeterminados. Si administra componentes de red desde afuera de un firewall, es posible que se le pida que vuelva a configurar el firewall para permitir el acceso en los puertos necesarios. Para obtener la lista de todos los puertos y protocolos compatibles en vCenter Server, consulte la herramienta VMware Ports and Protocols™ en https://ports.vmware.com/.

Durante la instalación, si un puerto se encuentra en uso o está bloqueado mediante una lista de no permitidos, el instalador de vCenter Server mostrará un mensaje de error. Debe utilizar otro número de puerto para continuar con la instalación.

VMware utiliza los puertos designados para la comunicación. Asimismo, los hosts administrados supervisan los puertos designados para los datos desde vCenter Server. Si existe un firewall integrado entre cualquiera de estos elementos, el instalador abre los puertos durante el proceso de instalación o actualización. En el caso de firewalls personalizados, debe abrir manualmente los puertos requeridos. Si posee un firewall entre dos hosts administrados y desea realizar actividades en el origen o destino, como la migración o clonación, debe configurar un medio para que los hosts administrados puedan recibir datos.

Para configurar el sistema vCenter Server a fin de que utilice un puerto diferente donde recibir los datos de vSphere Web Client, consulte la documentación de *Administrar vCenter Server y hosts*.

Requisitos de DNS para vCenter Server Appliance y el dispositivo de Platform Services Controller

Al implementar vCenter Server Appliance o el dispositivo de Platform Services Controller, de manera similar a cualquier servidor de red, es posible asignar una dirección IP fija y un FQDN que se pueda resolver mediante un servidor DNS, de modo que los clientes puedan acceder al servicio con confianza.

La implementación de vCenter Server Appliance o el dispositivo de Platform Services Controller con una dirección IP estática permite garantizar que la dirección IP del dispositivo siga siendo la misma en caso de que el sistema se reinicie.

Antes de implementar vCenter Server Appliance o el dispositivo de Platform Services Controller con una dirección IP estática, debe verificar que esta dirección IP tenga un registro de sistema de nombres de dominio (Domain Name System, DNS) interno válido.

Al implementar vCenter Server Appliance, la instalación del componente de servidor web que admite la instancia de vSphere Web Client genera un error si el instalador no puede buscar el nombre de dominio completo (FQDN) del dispositivo desde su dirección IP. La búsqueda inversa se implementa mediante registros PTR.

Si planea usar un FQDN para el nombre de sistema del dispositivo, debe comprobar que el FQDN pueda resolverse mediante un servidor DNS.

Se puede utilizar el comando `nslookup` para comprobar que el servicio de búsqueda inversa de DNS devuelva un FQDN cuando se realice una consulta con la dirección IP y que el FQDN pueda resolverse.

```
nslookup -nosearch -nodefname FQDN_or_IP_address
```

Si utiliza DHCP en lugar de una dirección IP estática para vCenter Server Appliance o un dispositivo de Platform Services Controller, compruebe que el nombre de dispositivo se actualice en el servicio de nombres de dominio (DNS). Si puede hacer ping al nombre del dispositivo; el nombre se actualiza en DNS.

Asegúrese de que la interfaz de administración del host ESXi tenga una resolución de DNS válida desde vCenter Server y todas las instancias de vSphere Web Client. Asegúrese de que vCenter Server tenga una resolución de DNS válida desde todos los hosts ESXi y todas las instancias de vSphere Web Client.

Requisitos de software de vSphere Web Client

Asegúrese de que su explorador sea compatible con vSphere Web Client.

vSphere Web Client 6.5 requiere Adobe Flash Player versión 16 a 23. Para obtener un mejor rendimiento y soluciones de seguridad, use Adobe Flash Player 23.

VMware ha probado y admite los siguientes sistemas operativos invitados y versiones de explorador para vSphere Web Client. Para obtener el mejor rendimiento, use Google Chrome.

Tabla 3-3. Sistemas operativos invitados compatibles y versiones de explorador mínimas para vSphere Web Client

Sistema operativo	Explorador
Windows de 32 bits y 64 bits	Microsoft Edge versión 79 a 86. Mozilla Firefox versión 60 a 84. Google Chrome versión 75 a 86.
Mac OS	Microsoft Edge versión 79 a 86. Mozilla Firefox versión 60 a 84. Google Chrome versión 75 a 86.

Prepararse para implementar vCenter Server Appliance y el dispositivo de Platform Services Controller

Antes de implementar vCenter Server Appliance o el dispositivo de Platform Services Controller, debe descargar el archivo ISO de instalación de vCenter Server Appliance y montarlo en la máquina virtual de red o en el servidor físico desde donde desea realizar la implementación.

El equipo desde el cual implementa el dispositivo se debe ejecutar en un sistema operativo Windows, Linux o Mac que cumpla con los requisitos del sistema operativo. Consulte Requisitos del sistema para el instalador de vCenter Server Appliance.

Requisitos del sistema para el instalador de vCenter Server Appliance

Puede ejecutar el instalador de GUI o CLI de vCenter Server Appliance desde un equipo cliente de red que se ejecuta en una versión compatible de un sistema operativo Windows, Linux o Mac.

Para garantizar el rendimiento óptimo de los instaladores de GUI y CLI, use un equipo cliente que cumpla con los requisitos mínimos de hardware.

Tabla 3-4. Requisitos del sistema para los instaladores de GUI y CLI

Sistema operativo	Versiones compatibles	Configuración de hardware mínima para un rendimiento óptimo
Windows	■ Windows 7, 8, 8.1, 10 ■ Windows 2012 de 64 bits ■ Windows 2012 R2 de 64 bits ■ Windows 2016 de 64 bits	4 GB de RAM, 2 CPU con 4 núcleos con 2,3 GHz, disco duro de 32 GB, 1 NIC
Linux	■ SUSE 12 ■ Ubuntu 14.04	4 GB de RAM, 1 CPU con 2 núcleos con 2,3 GHz, disco duro de 16 GB, 1 NIC **Nota** El instalador de CLI requiere un sistema operativo de 64 bits.
Mac	■ macOS v10.9, 10,10, 10.11 ■ macOS Sierra	8 GB de RAM, 1 CPU con 4 núcleos con 2,4 GHz, disco duro de 150 GB, 1 NIC

Nota Para los equipos cliente que se ejecutan en Mac 10.11, no se admiten las implementaciones de GUI simultáneas de varios dispositivos. Debe implementar los dispositivos en una secuencia.

Descargar y montar el instalador de vCenter Server Appliance

VMware lanzó la imagen ISO de vCenter Server Appliance, donde se incluyen los instaladores de GUI y CLI para vCenter Server Appliance y el dispositivo de Platform Services Controller.

Con los archivos ejecutables de GUI y CLI que se incluyen en el instalador de vCenter Server Appliance, es posible:

- Implementar vCenter Server Appliance y el dispositivo de Platform Services Controller.
- Actualizar vCenter Server Appliance y el dispositivo de Platform Services Controller.
- Migrar instalaciones en Windows de vCenter Server, vCenter Single Sign-On y Platform Services Controller a vCenter Server Appliance y el dispositivo de Platform Services Controller.
- Restaurar una instancia de vCenter Server Appliance de una copia de seguridad basada en archivos.

Requisitos previos

- Cree una cuenta de Customer Connect en https://my.vmware.com/web/vmware/.
- Compruebe que el equipo cliente cumpla con los requisitos del sistema para el instalador de vCenter Server Appliance. Consulte Requisitos del sistema para el instalador de vCenter Server Appliance.

Procedimiento

1. Inicie sesión en VMware Customer Connect.
2. Desplácese hasta **Productos y cuentas > Todos los productos**.
3. Busque VMware vSphere y haga clic en **Ver componentes de descarga**.
4. Seleccione una versión de VMware vSphere en el menú desplegable **Seleccionar versión**.
5. Seleccione una versión de VMware vCenter Server y haga clic en **IR A DESCARGAS**.
6. Descargue la imagen ISO de vCenter Server Appliance.
7. Confirme que md5sum sea correcto mediante una herramienta de suma de comprobación MD5.
8. Monte o extraiga la imagen ISO en el equipo cliente desde el cual desea implementar, actualizar, migrar o restaurar el dispositivo.

   Nota No se admite software de montaje o extracción de ISO en el que no se permitan más de ocho niveles de directorio.

   Por ejemplo, no se admite MagicISO Maker en Windows. No se admite Archive Manager en los sistemas operativos Linux y Mac.

   Se puede usar DiskImageMounter en el sistema operativo Mac.
   Se puede usar Disk Image Mounter en Ubuntu 14.04.
   Se puede usar el terminal en el sistema operativo SUSE 12.

   ```
   $ sudo mkdir mount_dir
   $ sudo mount -o loop VMware-vCSA-all-version_number-build_number.iso mount_dir
   ```

Pasos siguientes

Abra el archivo `readme.txt` y revise la información sobre los otros archivos y directorios en la imagen ISO de vCenter Server Appliance.

Sincronizar los relojes en la red de vSphere

Compruebe que todos los componentes de la red de vSphere tengan sus relojes sincronizados. Si los relojes de las máquinas de la red de vSphere no están sincronizados, los certificados SSL, que están sujetos a limitaciones temporales, pueden no reconocerse como válidos en las comunicaciones entre máquinas de la red.

Los relojes que no están sincronizados pueden ocasionar problemas de autenticación que, a su vez, pueden provocar que la instalación sea incorrecta o evitar que se inicie el servicio vpxd de vCenter Server Appliance.

Verifique que todos los equipos host de Windows en los que se ejecuta vCenter Server estén sincronizados con el servidor de tiempo de red (NTP). Consulte el artículo de la base de conocimientos http://kb.vmware.com/kb/1318.

Para sincronizar los relojes de ESXi con un servidor NTP, puede usar VMware Host Client. Para obtener información sobre cómo editar la configuración de hora de un host ESXi, consulte *Administrar un host único de vSphere*.

Requisitos previos para implementar vCenter Server Appliance o el dispositivo de Platform Services Controller

Para garantizar la correcta implementación de vCenter Server Appliance o el dispositivo de Platform Services Controller, es necesario realizar algunas tareas y comprobaciones previas obligatorias antes de ejecutar el instalador.

Requisitos previos generales

- Descargar y montar el instalador de vCenter Server Appliance.
- Para las topologías con instancias externas de Platform Services Controller, compruebe que la implementación de los distintos nodos se realice con sincronización de hora entre cada uno. Todas las instancias de vCenter Server, las instancias de Platform Services Controller y los equilibradores de carga de terceros del dominio de vCenter Single Sign-On deben contar con sincronización de hora. Consulte Sincronizar los relojes en la red de vSphere.

Requisitos previos de sistema de destino

- Compruebe que su sistema cumpla con los requisitos mínimos de hardware y software. Consulte Requisitos de sistema para el dispositivo vCenter Server Appliance y Platform Services Controller.
- Si desea implementar el dispositivo en un host ESXi, compruebe que el host ESXi no esté en modo de bloqueo o de mantenimiento y que no forme parte de un clúster de DRS completamente automatizado.
- Si planea implementar el dispositivo en un clúster de DRS en el inventario de una instancia de vCenter Server, compruebe que el clúster contenga al menos un host ESXi que no se encuentre en modo de bloqueo o de mantenimiento.
- Si desea utilizar servidores NTP para la sincronización de hora, compruebe que los servidores NTP estén en ejecución, y que la hora de esos servidores esté sincronizada con la del servidor de destino en el que desea implementar el dispositivo.

Requisitos previos de vCenter Enhanced Linked Mode

Al implementar una nueva instancia de vCenter Server como parte de una implementación de Enhanced Linked Mode, cree una copia de seguridad basada en imágenes de los nodos de vCenter Server existentes en el entorno. Puede utilizar la copia de seguridad como precaución en caso de que se produzca un error durante el proceso de implementación.

Si se produce un error en la implementación, elimine la instancia de vCenter Server Appliance recién implementada y restaure los nodos de vCenter Server a partir de sus respectivas copias de seguridad basadas en imágenes. Debe restaurar todos los nodos del entorno a partir de las copias de seguridad basadas en imágenes. Si no lo hace, es posible que los socios de replicación no estén sincronizados con el nodo restaurado.

- Para obtener más información sobre cómo crear implementaciones de vCenter Enhanced Linked Mode, consulte vCenter Enhanced Linked Mode.
- Para obtener información sobre las copias de seguridad basadas en imágenes, consulte Capítulo 7 Restaurar y crear copias de seguridad con base en imágenes de un entorno de vCenter Server.

Requisitos previos de red

Si desea asignar una dirección IP estática y un FQDN como nombre del sistema en la configuración de red del dispositivo, compruebe que se hayan configurado los registros de DNS inversos y directos para la dirección IP.

Implementación de la GUI de vCenter Server Appliance y del dispositivo de Platform Services Controller

Puede usar el instalador de GUI para realizar una implementación interactiva de vCenter Server Appliance con una instancia integrada de Platform Services Controller, un dispositivo de Platform Services Controller o una instancia de vCenter Server Appliance con una instancia externa de Platform Services Controller.

Al realizar la implementación de la GUI, debe descargar el instalador de vCenter Server Appliance en un equipo cliente de red, ejecutar el asistente de implementación desde el equipo cliente y proporcionar las entradas requeridas para implementar y configurar el dispositivo.

Importante Para usar topologías con instancias externas de Platform Services Controller, es necesario implementar las instancias de replicación de Platform Services Controller en secuencia. Después de implementar correctamente todas las instancias de Platform Services Controller en el dominio, se pueden realizar implementaciones simultáneas de varios dispositivos de vCenter Server que apuntan a una instancia externa común de Platform Services Controller.

El proceso de implementación de la GUI incluye una serie de dos etapas.

Figura 3-1. Etapa 1: Implementación de OVA



En la primera etapa, se utiliza el asistente de implementación para elegir el tipo de implementación y la configuración del dispositivo. En esta etapa, se completa la implementación del archivo OVA en el servidor de destino con el tipo de implementación y la configuración del dispositivo que se proporciona.

Como alternativa a la primera etapa de la implementación con el instalador de GUI, puede implementar el archivo OVA de vCenter Server Appliance o del dispositivo de Platform Services Controller mediante el uso de vSphere Web Client o VMware Host Client. Para implementar el archivo OVA en un host ESXio una instancia de vCenter Server 5.5 o 6.0, puede también usar vSphere Client. Después de la implementación de OVA, debe iniciar sesión en la interfaz de administración de dispositivos del dispositivo recientemente implementado para seguir con la segunda etapa del proceso de implementación.

Figura 3-2. Etapa 2: Configuración del dispositivo



En la segunda etapa, se utiliza el asistente de configuración para configurar la sincronización de hora del dispositivo y vCenter Single Sign-On. En esta etapa, finaliza la configuración inicial y se inician los servicios del dispositivo recientemente implementado.

Como alternativa a la segunda etapa de la implementación con el instalador de GUI, puede iniciar sesión en la interfaz de administración de dispositivos del dispositivo recientemente implementado, https://*FQDN_or_IP_address*:5480.

Información requerida para implementar una instancia de vCenter Server Appliance o un dispositivo de Platform Services Controller

Cuando se utiliza el método GUI para implementar una instancia de vCenter Server Appliance con una instancia integrada de Platform Services Controller, un dispositivo de Platform Services Controller o una instancia de vCenter Server Appliancecon una instancia externa de Platform Services Controller, el asistente solicita la información de implementación y configuración. Se recomienda mantener un registro de los valores introducidos por si debe reinstalar el producto.

Puede usar esta hoja de trabajo para registrar la información que necesita para implementar una instancia de vCenter Server Appliance con una instancia integrada de Platform Services Controller, un dispositivo de Platform Services Controller o una instancia de vCenter Server Appliance con una instancia externa de Platform Services Controller.

Tabla 3-5. Información requerida durante la etapa 1 del proceso de implementación de GUI

Requerida para la implementación de	Información necesaria	Predeterminado	Su entrada
Todos los tipos de implementación	El FQDN o la dirección IP del servidor de destino donde se desea implementar el dispositivo. El servidor de destino puede ser un host ESXi o una instancia de vCenter Server.	-	
	Puerto HTTPS del servidor de destino	443	
	Nombre de usuario con privilegios administrativos en el servidor de destino ■ Si el servidor de destino es un host ESXi, use el nombre de usuario raíz. ■ Si el servidor de destino es una instancia de vCenter Server, use *nombre_ de_ usuario@nombre_ de_ dominio*, por ejemplo, administrator@vsphere.local.	-	
	Contraseña del usuario con privilegios administrativos en el servidor de destino	-	
Todos los tipos de implementación Únicamente si el servidor de destino es una instancia de vCenter Server	Centro de datos del inventario de vCenter Server donde se desea implementar el dispositivo De manera opcional, puede proporcionar una carpeta para el centro de datos.	-	
	Host ESXi o clúster de DRS del inventario del centro de datos donde se desea implementar el dispositivo	-	
Todos los tipos de implementación	Nombre de la máquina virtual para el dispositivo ■ No debe contener signos de porcentaje (%), barras diagonales inversas (\) ni barras diagonales (/). ■ No debe tener más de 80 caracteres.	VMware vCenter Server Appliance	

Tabla 3-5. Información requerida durante la etapa 1 del proceso de implementación de GUI (continuación)

Requerida para la implementación de	Información necesaria	Predeterminado	Su entrada
Todos los tipos de implementación	Contraseña del usuario raíz del sistema operativo del dispositivo ■ Debe contener únicamente caracteres ASCII inferiores, sin espacios. ■ Debe contener al menos 8 caracteres y no más de 20. ■ Debe contener al menos una letra mayúscula. ■ Debe contener al menos una letra minúscula. ■ Debe contener al menos un número. ■ Debe contener al menos un carácter especial, por ejemplo, un signo de dólar ($), un numeral (#), una arroba (@), un punto (.) o un signo de exclamación (!).	-	

Tabla 3-5. Información requerida durante la etapa 1 del proceso de implementación de GUI (continuación)

Requerida para la implementación de	Información necesaria	Predeterminado	Su entrada
■ vCenter Server Appliance con una instancia de Platform Services Controller integrada ■ vCenter Server Appliance con una instancia de Platform Services Controller externa	Tamaño de implementación de la instancia de vCenter Server Appliance para el entorno de vSphere ■ Muy pequeño Implementa un dispositivo con 2 CPU y 10 GB de memoria. Apropiado para entornos con hasta 10 hosts o 100 máquinas virtuales. ■ Pequeño Implementa un dispositivo con 4 CPU y 16 GB de memoria. Apropiado para entornos con hasta 100 hosts o 1.000 máquinas virtuales. ■ Mediano Implementa un dispositivo con 8 CPU y 24 GB de memoria. Apropiado para entornos con hasta 400 hosts o 4.000 máquinas virtuales. ■ Grande Implementa un dispositivo con 16 CPU y 32 GB de memoria. Apropiado para entornos con hasta 1.000 hosts o 10.000 máquinas virtuales. ■ Extra grande Implementa un dispositivo con 24 CPU y 48 GB de memoria. Apropiado para entornos con hasta 2.000 hosts o 35.000 máquinas virtuales.	Muy pequeño	

Tabla 3-5. Información requerida durante la etapa 1 del proceso de implementación de GUI (continuación)

Requerida para la implementación de	Información necesaria	Predeterminado	Su entrada
■ vCenter Server Appliance con una instancia de Platform Services Controller integrada ■ vCenter Server Appliance con una instancia de Platform Services Controller externa	Tamaño de almacenamiento de la instancia de vCenter Server Appliance para el entorno de vSphere Incremente el tamaño de almacenamiento predeterminado si desea un volumen mayor para datos SEAT (estadísticas, eventos, alarmas y tareas). ■ Predeterminado Para el tamaño de implementación muy pequeño, implementa el dispositivo con 250 GB de almacenamiento. Para el tamaño de implementación pequeño, implementa el dispositivo con 290 GB de almacenamiento. Para el tamaño de implementación mediano, implementa el dispositivo con 425 GB de almacenamiento. Para el tamaño de implementación grande, implementa el dispositivo con 640 GB de almacenamiento. Para el tamaño de implementación extragrande, implementa el dispositivo con 980 GB de almacenamiento. ■ Grande Para el tamaño de implementación muy pequeño, implementa el dispositivo con 775 GB de almacenamiento. Para el tamaño de implementación pequeño, implementa el dispositivo con 820 GB de almacenamiento. Para el tamaño de implementación mediano, implementa el dispositivo con 925 GB de almacenamiento.	Predeterminado	

Tabla 3-5. Información requerida durante la etapa 1 del proceso de implementación de GUI (continuación)

Requerida para la implementación de	Información necesaria	Predeterminado	Su entrada
	Para el tamaño de implementación grande, implementa el dispositivo con 990 GB de almacenamiento. Para el tamaño de implementación extragrande, implementa el dispositivo con 1.030 GB de almacenamiento. ■ Extra grande Para el tamaño de implementación muy pequeño, implementa el dispositivo con 1.650 GB de almacenamiento. Para el tamaño de implementación pequeño, implementa el dispositivo con 1.700 GB de almacenamiento. Para el tamaño de implementación mediano, implementa el dispositivo con 1.805 GB de almacenamiento. Para el tamaño de implementación grande, implementa el dispositivo con 1.870 GB de almacenamiento. Para el tamaño de implementación extragrande, implementa el dispositivo con 1.910 GB de almacenamiento.		
Todos los tipos de implementación	Nombre del almacén de datos donde se desean almacenar los archivos de configuración y los discos virtuales del dispositivo **Nota** El instalador muestra una lista de almacenes de datos a los que se puede acceder desde el servidor de destino.	-	
	Habilitar o deshabilitar el modo de disco fino	Deshabilitado	

Tabla 3-5. Información requerida durante la etapa 1 del proceso de implementación de GUI (continuación)

Requerida para la implementación de	Información necesaria	Predeterminado	Su entrada
Todos los tipos de implementación	Nombre de la red a la que se conectará el dispositivo **Nota** El instalador muestra un menú desplegable con redes que dependen de la configuración de red del servidor de destino. En el caso de la implementación directa de un dispositivo en un host ESXi, los grupos de puertos virtuales distribuidos que no son efímeros no se admiten y no se muestran en el menú desplegable. Debe poder accederse a la red desde el equipo cliente donde se realiza la implementación.	-	
	Versión IP de la dirección del dispositivo Puede ser IPv4 o IPv6.	IPv4	
	Asignación de direcciones IP de la dirección del dispositivo Puede ser estática o DHCP.	estático	
Todos los tipos de implementación Solo si se utiliza una asignación estática	Nombre del sistema (FQDN o dirección IP) El nombre del sistema se utiliza para administrar el sistema local. El nombre del sistema debe ser FQDN. Si no hay un servidor DNS disponible, proporcione una dirección IP estática.	-	
	Dirección IP	-	
	Para la versión IPv4, una máscara de subred como notación decimal con punto o un prefijo de red como número entero entre 0 y 32 Para la versión IPv6, un prefijo de red como número entero entre 0 y 128	-	
	Puerta de enlace predeterminada	-	

Tabla 3-5. Información requerida durante la etapa 1 del proceso de implementación de GUI (continuación)

Requerida para la implementación de	Información necesaria	Predeterminado	Su entrada
	Servidores DNS separados por comas	-	
Todos los tipos de implementación Solo si utiliza DHCP con IPv4 y tiene un servidor DNS dinámico (DDNS) disponible en su entorno.	Nombre del sistema (FQDN)	-	

Tabla 3-6. Información requerida durante la etapa 2 del proceso de implementación de GUI

Necesario para	Información necesaria	Predeterminado	Su entrada
Todos los tipos de implementación	Configuración de sincronización de hora Puede sincronizar la hora del dispositivo con la hora del host ESXi o con uno o varios servidores NTP. Si desea usar más de un servidor NTP, debe proporcionar las direcciones IP o FQDN de los servidores NTP como lista separada por comas.	Sincronizar la hora con los servidores NTP	
	Habilitar o deshabilitar el acceso SSH **Nota** vCenter Server Appliance de alta disponibilidad requiere acceso SSH remoto al dispositivo.	Deshabilitado	
■ vCenter Server Appliance con una instancia de Platform Services Controller integrada ■ El dispositivo de Platform Services Controller como la primera instancia en un dominio nuevo	Nombre del nuevo dominio de vCenter Single Sign-On Por ejemplo, vsphere.local.	-	

Tabla 3-6. Información requerida durante la etapa 2 del proceso de implementación de GUI (continuación)

<table>
<tr><th>Necesario para</th><th>Información necesaria</th><th>Predeterminado</th><th>Su entrada</th></tr>
<tr><td rowspan="2"></td><td>Contraseña de la cuenta de administrador, administrator@nombre_del_dominio.
Debe contener al menos 8 caracteres y no más de 20.
Debe contener al menos una letra mayúscula.
Debe contener al menos una letra minúscula.
Debe contener al menos un número.
Debe contener al menos un carácter especial, como una y comercial (&), una almohadilla (#) y el signo de porcentaje (%)</td><td>-</td><td></td></tr>
<tr><td>Nombre del sitio</td><td>-</td><td></td></tr>
<tr><td rowspan="4">vCenter Server Appliance con una instancia de Platform Services Controller externa
El dispositivo de Platform Services Controller como instancia posterior en un dominio existente</td><td>FQDN o dirección IP de la instancia de Platform Services Controller a la que desea unirse
Debe unirse a una instancia de Platform Services Controller de la misma versión.</td><td>-</td><td></td></tr>
<tr><td>Puerto HTTPS de la instancia de Platform Services Controller</td><td>443</td><td></td></tr>
<tr><td>Nombre de dominio de vCenter Single Sign On de la instancia de Platform Services Controller
Por ejemplo, vsphere.local.</td><td>-</td><td></td></tr>
<tr><td>Contraseña del usuario administrador de vCenter Single Sign On para el dominio</td><td>-</td><td></td></tr>
</table>

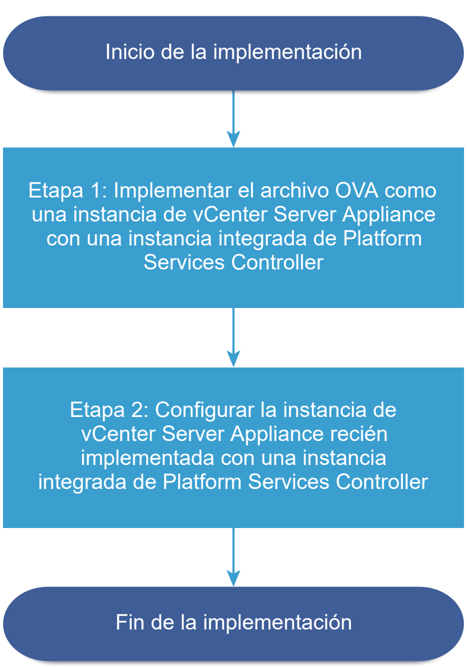
Tabla 3-6. Información requerida durante la etapa 2 del proceso de implementación de GUI (continuación)

Necesario para	Información necesaria	Predeterminado	Su entrada
	Nombre del sitio de vCenter Single Sign-On Puede unirse a un sitio existente o crear uno nuevo.	-	
■ vCenter Server Appliance con una instancia de Platform Services Controller integrada ■ Dispositivo de Platform Services Controller	Decida si desea unirse al Programa de mejora de la experiencia del cliente (Customer Experience Improvement Program, CEIP) de VMware Para obtener más información sobre el CEIP, consulte la sección Configurar el Programa de mejora de la experiencia del cliente en *Administrar vCenter Server y hosts*.	Unirse al CEIP	

Implementar vCenter Server Appliance con una instancia integrada de Platform Services Controller mediante la GUI

Es posible utilizar el instalador de GUI para ejecutar una implementación interactiva de vCenter Server Appliance con una instancia integrada de Platform Services Controller. Se debe ejecutar la implementación de GUI desde un equipo Windows, Linux o Mac que se encuentre en la misma red en la que se desea implementar el dispositivo.

Figura 3-3. Flujo de trabajo de implementación de vCenter Server Appliance con una instancia integrada de Platform Services Controller



Requisitos previos

- Consulte Requisitos previos para implementar vCenter Server Appliance o el dispositivo de Platform Services Controller.
- Consulte Información requerida para implementar una instancia de vCenter Server Appliance o un dispositivo de Platform Services Controller.

Procedimiento

1 Etapa 1: Implementar el archivo OVA como vCenter Server Appliance con una instancia integrada de Platform Services Controller

La etapa 1 del proceso de implementación permite implementar el archivo OVA, que se incluye en el instalador de vCenter Server Appliance, como vCenter Server Appliance con una instancia integrada de Platform Services Controller.

2 Etapa 2 - Configure la instancia de vCenter Server Appliance recién implementada con Platform Services Controller integrado

Cuando la implementación de OVA termina, se le redirige a la etapa 2 del proceso de implementación para que configure e inicie los servicios de la instancia de vCenter Server Appliance recién implementada con Platform Services Controller integrado.

Etapa 1: Implementar el archivo OVA como vCenter Server Appliance con una instancia integrada de Platform Services Controller

La etapa 1 del proceso de implementación permite implementar el archivo OVA, que se incluye en el instalador de vCenter Server Appliance, como vCenter Server Appliance con una instancia integrada de Platform Services Controller.

Procedimiento

1 En el instalador de vCenter Server Appliance, desplácese hasta el directorio `vcsa-ui-installer`, vaya al subdirectorio del sistema operativo y ejecute el instalador.

- En un sistema operativo Windows, vaya al subdirectorio `win32` y ejecute el archivo `installer.exe`.
- En un sistema operativo Linux, vaya al subdirectorio `lin64` y ejecute el archivo `installer`.
- En un sistema operativo Mac OS, vaya al subdirectorio `mac` y ejecute el archivo `Installer.app`.

2 En la página de inicio, haga clic en **Instalar** para iniciar el asistente de implementación.

3 Revise la página de introducción para comprender el proceso de implementación y haga clic en **Siguiente**.

4 Lea y acepte el contrato de licencia, y haga clic en **Siguiente**.

5 En la página Seleccionar tipo de implementación, seleccione **vCenter Server con una instancia integrada de Platform Services Controller** y haga clic en **Siguiente**.

Esta opción implementa una aplicación en la que están instalados Platform Services Controller y también vCenter Server.

6 Conéctese al servidor de destino donde desea implementar vCenter Server Appliance.

Opción	Pasos
Puede conectarse a un host ESXi para implementar el dispositivo allí.	1 Escriba el FQDN o la dirección IP del host ESXi. 2 Especifique el puerto HTTPS del host ESXi. 3 Escriba el nombre de usuario y la contraseña de un usuario que tenga privilegios administrativos en el host ESXi (por ejemplo, el usuario raíz). 4 Haga clic en **Siguiente**. 5 Asegúrese de que la advertencia de certificado muestre la huella digital SHA1 del certificado SSL que se instaló en el host ESXi de destino y haga clic en **Sí** para aceptar la huella digital del certificado.
Puede conectarse a una instancia de vCenter Server y examinar el inventario para seleccionar un host ESXi o un clúster de DRS donde se implementará el dispositivo.	1 Escriba el nombre de dominio completo o la dirección IP de la instancia de vCenter Server. 2 Especifique el puerto HTTPS de la instancia de vCenter Server. 3 Especifique el nombre de usuario y la contraseña de un usuario con privilegios administrativos de vCenter Single Sign-On en la instancia de vCenter Server (por ejemplo, el usuario administrator@*su_nombre_de_dominio*). 4 Haga clic en **Siguiente**. 5 Asegúrese de que la advertencia de certificado muestre la huella digital SHA1 del certificado SSL que se instaló en la instancia de vCenter Server de destino y haga clic en **Sí** para aceptar la huella digital del certificado. 6 Seleccione el centro de datos o la carpeta de centro de datos que contiene el host ESXi o el clúster de DRS donde desea implementar el dispositivo y haga clic en **Siguiente**. **Nota** Es necesario seleccionar un centro de datos o una carpeta de centro de datos que contenga al menos un host ESXi que no se encuentre en modo de bloqueo o de mantenimiento. 7 Seleccione el host ESXi o el clúster de DRS donde desea implementar el dispositivo y haga clic en **Siguiente**.

7 En la página Configurar máquina virtual de dispositivo, escriba un nombre para vCenter Server Appliance, establezca la contraseña del usuario raíz y haga clic en **Siguiente**.

El nombre del dispositivo no debe contener ningún signo de porcentaje (%), ninguna barra inversa (\) ni ninguna barra diagonal (/), y tampoco debe tener más de 80 caracteres.

La contraseña debe contener solo caracteres ASCII inferiores sin espacios, al menos ocho caracteres, un número, letras minúsculas y mayúsculas, y un carácter especial, por ejemplo, un signo de exclamación (!), un numeral (#), una arroba (@) o un paréntesis (()).

8 Seleccione el tamaño de la implementación para la instancia de vCenter Server Appliance de su inventario de vSphere.

Opción de tamaño de implementación	Descripción
Muy pequeño	Implementa un dispositivo con 2 CPU y 10 GB de memoria. Apropiado para entornos con hasta 10 hosts o 100 máquinas virtuales.
Pequeño	Implementa un dispositivo con 4 CPU y 16 GB de memoria. Apropiado para entornos con hasta 100 hosts o 1.000 máquinas virtuales.
Mediano	Implementa un dispositivo con 8 CPU y 24 GB de memoria. Apropiado para entornos con hasta 400 hosts o 4.000 máquinas virtuales.
Grande	Implementa un dispositivo con 16 CPU y 32 GB de memoria. Apropiado para entornos con hasta 1.000 hosts o 10.000 máquinas virtuales.
Extra grande	Implementa un dispositivo con 24 CPU y 48 GB de memoria. Apropiado para entornos con hasta 2.000 hosts o 35.000 máquinas virtuales.

9 Seleccione el tamaño de almacenamiento de vCenter Server Appliance y haga clic en **Siguiente**.

Opción de tamaño de almacenamiento	Descripción de tamaño de implementación muy pequeño	Descripción de tamaño de implementación pequeño	Descripción de tamaño de implementación mediano	Descripción de tamaño de implementación grande	Descripción de tamaño de implementación extragrande
Predeterminado	Implementa un dispositivo con 250 GB de almacenamiento.	Implementa un dispositivo con 290 GB de almacenamiento.	Implementa un dispositivo con 425 GB de almacenamiento.	Implementa un dispositivo con 640 GB de almacenamiento.	Implementa un dispositivo con 980 GB de almacenamiento.
Grande	Implementa un dispositivo con 775 GB de almacenamiento.	Implementa un dispositivo con 820 GB de almacenamiento.	Implementa un dispositivo con 925 GB de almacenamiento.	Implementa un dispositivo con 990 GB de almacenamiento.	Implementa un dispositivo con 1.030 GB de almacenamiento.
Extragrande	Implementa un dispositivo con 1.650 GB de almacenamiento.	Implementa un dispositivo con 1.700 GB de almacenamiento.	Implementa un dispositivo con 1.805 GB de almacenamiento.	Implementa un dispositivo con 1.870 GB de almacenamiento.	Implementa un dispositivo con 1.910 GB de almacenamiento.

10 En la lista de almacenes de datos disponibles, seleccione la ubicación en la que se almacenarán todos los archivos de configuración y discos virtuales de la máquina virtual. Opcionalmente, seleccione **Habilitar el modo de disco fino** para habilitar el aprovisionamiento fino.

11 En la página Ajustar la configuración de red, establezca la configuración de red.

La dirección IP o el FQDN del dispositivo se utilizan como nombre del sistema. Se recomienda utilizar un FQDN. Sin embargo, si desea utilizar una dirección IP, utilice asignación de direcciones IP estáticas del dispositivo, ya que las direcciones IP que asigna DHCP podrían cambiar.

Opción	Acción
Red	Seleccione la red a la que desea conectar el dispositivo. Las redes que se muestran en el menú desplegable dependen de la configuración de red del servidor de destino. En el caso de la implementación directa de un dispositivo en un host ESXi, los grupos de puertos virtuales distribuidos que no son efímeros no se admiten y no se muestran en el menú desplegable.
Versión IP	Seleccione la versión de la dirección IP del dispositivo. Puede seleccionar la versión IPv4 o IPv6.
Asignación de IP	Seleccione cómo asignar la dirección IP del dispositivo. ■ **estático** El asistente solicita que se introduzca la dirección IP y la configuración de red. **Nota** Evite utilizar una dirección IP como nombre del sistema. Si utiliza una dirección IP como nombre del sistema, no podrá cambiar la dirección IP ni actualizar la configuración de DNS después de la implementación; tampoco podrá unir el dispositivo a un dominio de Active Directory. ■ **DHCP** Los servidores DHCP se utilizan para asignar la dirección IP. Seleccione esta opción solo si hay un servidor DHCP disponible en el entorno. Si hay un DDNS habilitado en el entorno, puede escribir el nombre de dominio completo (Fully qualified domain name, FQDN) que prefiera para el dispositivo.
Puertos comunes	Puede personalizar los puertos HTTP y HTTPS (opcional). Si se especifican números de puerto HTTP y HTTPS personalizados, asegúrese de usar números de puerto que no se usen en vCenter Server, así como de evitar utilizar los puertos HTTP y HTTPS predeterminados (80 y 443). **Nota** Los puertos personalizados son compatibles a partir de vSphere 6.5 Update 2.

12 En la página Listo para finalizar la etapa 1, revise la configuración de implementación de vCenter Server Appliance y haga clic en **Finalizar** para iniciar el proceso de implementación de OVA.

13 Espere a que finalice la implementación de OVA y haga clic en **Continuar** para pasar a la etapa 2 del proceso de implementación a fin de configurar e iniciar los servicios del dispositivo recién implementado.

Nota Si hace clic en **Cerrar** para salir del asistente, deberá iniciar sesión en la interfaz de administración de vCenter Server Appliance para configurar e iniciar los servicios.

Resultados

La instancia de vCenter Server Appliance recién implementada con una instancia integrada de Platform Services Controller se ejecuta en el servidor de destino, pero los servicios no están iniciados.

Etapa 2 - Configure la instancia de vCenter Server Appliance recién implementada con Platform Services Controller integrado

Cuando la implementación de OVA termina, se le redirige a la etapa 2 del proceso de implementación para que configure e inicie los servicios de la instancia de vCenter Server Appliance recién implementada con Platform Services Controller integrado.

Procedimiento

1 Revise la introducción a la etapa 2 del proceso de implementación y haga clic en **Siguiente**.

2 Ajuste la configuración de la hora en el dispositivo. De manera opcional, habilite el acceso SSH remoto al dispositivo y haga clic en **Siguiente**.

Opción	Descripción
Sincronizar la hora con el host ESXi	Habilita la sincronización horaria periódica y permite que VMware Tools establezca la hora del sistema operativo invitado para que sea la misma que la hora del host ESXi.
Sincronizar la hora con los servidores NTP	Utiliza un servidor de protocolo de tiempo de red para sincronizar la hora. Si selecciona esta opción, deberá escribir los nombres o las direcciones IP de los servidores NTP separados por comas.

3 Cree un nuevo dominio de vCenter Single Sign-On o únase a un dominio existente.

Opción	Descripción
Crear un nuevo dominio de Single Sign-On	Crea un nuevo dominio de vCenter Single Sign-On. a Introduzca el nombre de dominio; por ejemplo, **`vsphere.local`**. b Establezca el nombre de usuario de la cuenta de administrador de vCenter Single Sign-On, por ejemplo, **`administrator`**. Después de la implementación, puede iniciar sesión en vCenter Single Sign-On y en vCenter Server como *adminstrator_user_name@su_nombre_de_dominio*. c Defina la contraseña para la cuenta de administrador de vCenter Single Sign-On. Esta es la contraseña del usuario *adminstrator_user_name@su_nombre_de_dominio*. d Introduzca el nombre del sitio para vCenter Single Sign-On. El nombre del sitio es importante si utiliza vCenter Single Sign-On en varias ubicaciones. El nombre del sitio debe contener caracteres alfanuméricos. Seleccione su propio nombre para el sitio de vCenter Single Sign-On. No puede cambiar el nombre después de la instalación. En los nombres de sitio no se admiten caracteres ASCII extendidos ni caracteres que no sean ASCII. Igualmente, deben incluir caracteres alfanuméricos y coma (,), punto (.), signo de interrogación (?), guion (-), guion bajo (_), signo más (+) o signo igual (=). **Nota** Al configurar una instancia de Embedded Linked Mode, utilice **`Primer sitio predeterminado`** como el nombre del sitio para la primera instancia. e Haga clic en **Siguiente**.
Unirse a un dominio de vCenter Single Sign-On existente	Se une a un nuevo servidor vCenter Single Sign-On a un dominio de vCenter Single Sign-On en una instancia de Platform Services Controller existente. Debe proporcionar la información sobre el servidor vCenter Single Sign-On al que se va a unir el nuevo servidor vCenter Single Sign-On. a Escriba el nombre de dominio completo (fully qualified domain name, FQDN) o la dirección IP de la instancia de Platform Services Controller que contiene el servidor vCenter Single Sign-On al que se va a unir. b Introduzca el puerto HTTPS que se usará para la comunicación con Platform Services Controller. c Escriba el nombre de usuario y la contraseña de la cuenta de administrador de vCenter Single Sign-On. d Haga clic en **Siguiente**. e Apruebe el certificado que brinda el equipo remoto y determine si desea crear un sitio de vCenter Single Sign-On o unirse a uno existente. f Determine si desea crear un sitio de vCenter Single Sign-On o unirse a uno existente.

4 Revise la página del Programa de mejora de la experiencia del cliente (Customer Experience Improvement Program, CEIP) de VMware y decida si desea unirse a él.

   Para obtener más información sobre el CEIP, consulte la sección Configurar el Programa de mejora de la experiencia del cliente en *Administrar vCenter Server y hosts*.

5 En la página Listo para finalizar, revise los ajustes de configuración de vCenter Server Appliance, y haga clic en **Finalizar** y en **Aceptar** para completar la etapa 2 del proceso de implementación y configurar el dispositivo.

6 (opcional) Cuando termine la configuración inicial, haga clic en **https://*vcenter_server_appliance_fqdn*/vsphere-client** para ir a vSphere Web Client e inicie sesión en la instancia de vCenter Server de vCenter Server Appliance, o bien haga clic en **https://*vcenter_server_appliance_fqdn*:443** para ir a la página de introducción de vCenter Server Appliance.

7 Haga clic en **Cerrar** para cerrar el asistente.

   Se abrirá la página de introducción de vCenter Server Appliance.

Pasos siguientes

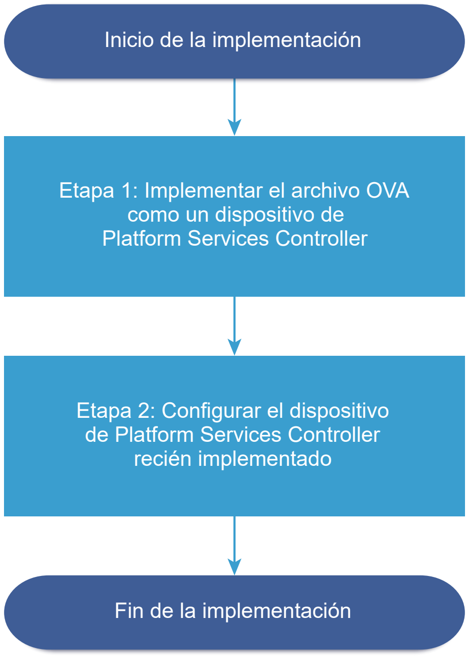
Es posible configurar la alta disponibilidad para vCenter Server Appliance. Para obtener información sobre la forma de proporcionar alta disponibilidad a vCenter Server Appliance, consulte *Disponibilidad de vSphere*.

Actualizar un dispositivo de Platform Services Controller mediante la GUI

Puede utilizar el instalador de la GUI para realizar una implementación interactiva de un dispositivo de Platform Services Controller como primera instancia de un nuevo dominio de vCenter Single Sign-On o como partner de replicación en un dominio de vCenter Single Sign-On existente.
Se debe ejecutar la implementación de GUI desde un equipo Windows, Linux o Mac que se encuentre en la misma red en la que se desea implementar el dispositivo.

Importante Debe implementar las instancias de replicación de Platform Services Controller en una secuencia.

Figura 3-4. Flujo de trabajo de implementación de un dispositivo de Platform Services Controller



Requisitos previos

- Consulte Requisitos previos para implementar vCenter Server Appliance o el dispositivo de Platform Services Controller.
- Consulte Información requerida para implementar una instancia de vCenter Server Appliance o un dispositivo de Platform Services Controller.

Procedimiento

1 Etapa 1: Implementar el archivo OVA como dispositivo de Platform Services Controller

  En la etapa 1 del proceso de implementación, se implementa el archivo OVA, que está incluido en el instalador de vCenter Server Appliance como dispositivo de Platform Services Controller.

2 Etapa 2: Configurar el dispositivo de Platform Services Controller recién implementado

  Cuando finalice la implementación de OVA, se lo redireccionará a la etapa 2 del proceso de implementación para configurar e iniciar los servicios del dispositivo de Platform Services Controller recién implementado.

Etapa 1: Implementar el archivo OVA como dispositivo de Platform Services Controller

En la etapa 1 del proceso de implementación, se implementa el archivo OVA, que está incluido en el instalador de vCenter Server Appliance como dispositivo de Platform Services Controller.

Procedimiento

1 En el instalador de vCenter Server Appliance, desplácese hasta el directorio `vcsa-ui-installer`, vaya al subdirectorio del sistema operativo y ejecute el instalador.

    - En un sistema operativo Windows, vaya al subdirectorio `win32` y ejecute el archivo `installer.exe`.
    - En un sistema operativo Linux, vaya al subdirectorio `lin64` y ejecute el archivo `installer`.
    - En un sistema operativo Mac OS, vaya al subdirectorio `mac` y ejecute el archivo `Installer.app`.

2 En la página de inicio, haga clic en **Instalar** para iniciar el asistente de implementación.

3 Revise la página de introducción para comprender el proceso de implementación y haga clic en **Siguiente**.

4 Lea y acepte el contrato de licencia, y haga clic en **Siguiente**.

5 En la página Seleccionar un tipo de implementación, seleccione **Platform Services Controller** y haga clic en **Siguiente**.

6 Conéctese al servidor de destino en el cual desea implementar el dispositivo de Platform Services Controller y haga clic en **Siguiente**.

Opción	Pasos
Puede conectarse a un host ESXi para implementar el dispositivo allí.	1 Escriba el FQDN o la dirección IP del host ESXi. 2 Especifique el puerto HTTPS del host ESXi. 3 Escriba el nombre de usuario y la contraseña de un usuario que tenga privilegios administrativos en el host ESXi (por ejemplo, el usuario raíz). 4 Haga clic en **Siguiente**. 5 Asegúrese de que la advertencia de certificado muestre la huella digital SHA1 del certificado SSL que se instaló en el host ESXi de destino y haga clic en **Sí** para aceptar la huella digital del certificado.
Puede conectarse a una instancia de vCenter Server y examinar el inventario para seleccionar un host ESXi o un clúster de DRS donde se implementará el dispositivo.	1 Escriba el nombre de dominio completo o la dirección IP de la instancia de vCenter Server. 2 Especifique el puerto HTTPS de la instancia de vCenter Server. 3 Especifique el nombre de usuario y la contraseña de un usuario con privilegios administrativos de vCenter Single Sign-On en la instancia de vCenter Server (por ejemplo, el usuario administrator@*su_nombre_de_dominio*). 4 Haga clic en **Siguiente**. 5 Asegúrese de que la advertencia de certificado muestre la huella digital SHA1 del certificado SSL que se instaló en la instancia de vCenter Server de destino y haga clic en **Sí** para aceptar la huella digital del certificado. 6 Seleccione el centro de datos o la carpeta de centro de datos que contiene el host ESXi o el clúster de DRS donde desea implementar el dispositivo y haga clic en **Siguiente**. **Nota** Es necesario seleccionar un centro de datos o una carpeta de centro de datos que contenga al menos un host ESXi que no se encuentre en modo de bloqueo o de mantenimiento. 7 Seleccione el host ESXi o el clúster de DRS donde desea implementar el dispositivo y haga clic en **Siguiente**.

7 En la página Configurar máquina virtual de dispositivo, escriba un nombre para el dispositivo de Platform Services Controller, establezca la contraseña del usuario raíz y haga clic en **Siguiente**.

El nombre del dispositivo no debe contener ningún signo de porcentaje (%), ninguna barra inversa (\) ni ninguna barra diagonal (/), y tampoco debe tener más de 80 caracteres.

La contraseña debe contener solo caracteres ASCII inferiores sin espacios, al menos ocho caracteres, un número, letras minúsculas y mayúsculas, y un carácter especial, por ejemplo, un signo de exclamación (!), un numeral (#), una arroba (@) o un paréntesis (()).

8 En la lista de almacenes de datos disponibles, seleccione la ubicación en la que se almacenarán todos los archivos de configuración y discos virtuales de la máquina virtual. Opcionalmente, seleccione **Habilitar el modo de disco fino** para habilitar el aprovisionamiento fino.

9 En la página Ajustar la configuración de red, establezca la configuración de red.

La dirección IP o el FQDN del dispositivo se utilizan como nombre del sistema. Se recomienda utilizar un FQDN. Sin embargo, si desea utilizar una dirección IP, utilice asignación de direcciones IP estáticas del dispositivo, ya que las direcciones IP que asigna DHCP podrían cambiar.

Opción	Acción
Red	Seleccione la red a la que desea conectar el dispositivo. Las redes que se muestran en el menú desplegable dependen de la configuración de red del servidor de destino. En el caso de la implementación directa de un dispositivo en un host ESXi, los grupos de puertos virtuales distribuidos que no son efímeros no se admiten y no se muestran en el menú desplegable.
Versión IP	Seleccione la versión de la dirección IP del dispositivo. Puede seleccionar la versión IPv4 o IPv6.
Asignación de IP	Seleccione cómo asignar la dirección IP del dispositivo. ■ **estático** El asistente solicita que se introduzca la dirección IP y la configuración de red. **Nota** Evite utilizar una dirección IP como nombre del sistema. Si utiliza una dirección IP como nombre del sistema, no podrá cambiar la dirección IP ni actualizar la configuración de DNS después de la implementación; tampoco podrá unir el dispositivo a un dominio de Active Directory. ■ **DHCP** Los servidores DHCP se utilizan para asignar la dirección IP. Seleccione esta opción solo si hay un servidor DHCP disponible en el entorno. Si hay un DDNS habilitado en el entorno, puede escribir el nombre de dominio completo (Fully qualified domain name, FQDN) que prefiera para el dispositivo.
Puertos comunes	Puede personalizar los puertos HTTP y HTTPS (opcional). Si se especifican números de puerto HTTP y HTTPS personalizados, asegúrese de usar números de puerto que no se usen en vCenter Server, así como de evitar utilizar los puertos HTTP y HTTPS predeterminados (80 y 443). **Nota** Los puertos personalizados son compatibles a partir de vSphere 6.5 Update 2.

10 En la página Listo para finalizar la etapa 1, revise la configuración de implementación del dispositivo de Platform Services Controller y haga clic en **Finalizar** para iniciar el proceso de implementación de OVA.

11 Espere a que finalice la implementación de OVA y haga clic en **Continuar** para pasar a la etapa 2 del proceso de implementación a fin de configurar e iniciar los servicios del dispositivo recién implementado.

Nota Si hace clic en **Cerrar** para salir del asistente, deberá iniciar sesión en la interfaz de administración del dispositivo de Platform Services Controller para configurar e iniciar los servicios.

Resultados

El dispositivo de Platform Services Controller recién implementado está en ejecución en el servidor de destino, pero no se inician los servicios.

Etapa 2: Configurar el dispositivo de Platform Services Controller recién implementado

Cuando finalice la implementación de OVA, se lo redireccionará a la etapa 2 del proceso de implementación para configurar e iniciar los servicios del dispositivo de Platform Services Controller recién implementado.

Procedimiento

1 Revise la introducción a la etapa 2 del proceso de implementación y haga clic en **Siguiente**.

2 Ajuste la configuración de la hora en el dispositivo. De manera opcional, habilite el acceso SSH remoto al dispositivo y haga clic en **Siguiente**.

Opción	Descripción
Sincronizar la hora con el host ESXi	Habilita la sincronización horaria periódica y permite que VMware Tools establezca la hora del sistema operativo invitado para que sea la misma que la hora del host ESXi.
Sincronizar la hora con los servidores NTP	Utiliza un servidor de protocolo de tiempo de red para sincronizar la hora. Si selecciona esta opción, deberá escribir los nombres o las direcciones IP de los servidores NTP separados por comas.

3 Cree un nuevo dominio de vCenter Single Sign-On o únase a un dominio existente.

Opción	Descripción
Crear un nuevo dominio de Single Sign-On	Crea un dominio de vCenter Single Sign-On. a Introduzca el nombre de dominio; por ejemplo, `vsphere.local`. b Defina la contraseña para la cuenta de administrador de vCenter Single Sign-On. Esta es la contraseña del usuario administrator@*su_nombre_de_dominio*. c Introduzca el nombre del sitio para vCenter Single Sign-On. El nombre del sitio es importante si utiliza vCenter Single Sign-On en varias ubicaciones. El nombre del sitio debe contener caracteres alfanuméricos. Seleccione su propio nombre para el sitio de vCenter Single Sign-On. No puede cambiar el nombre después de la instalación. En los nombres de sitio no se admiten caracteres ASCII extendidos ni caracteres que no sean ASCII. Igualmente, deben incluir caracteres alfanuméricos y coma (,), punto (.), signo de interrogación (?), guion (-), guion bajo (_), signo más (+) o signo igual (=). d Haga clic en **Siguiente**.
Unirse a un dominio de vCenter Single Sign-On existente	Une el dispositivo de Platform Services Controller a un dominio de vCenter Single Sign-On existente como partner de replicación de una instancia de Platform Services Controller actual. Debe proporcionar información acerca de la instancia de Platform Services Controller del partner al que desea unirse. a Introduzca el FQDN o la dirección IP de la instancia de Platform Services Controller del partner. b Introduzca el puerto HTTPS de la instancia de Platform Services Controller del partner. c Introduzca el nombre de dominio de vCenter Single Sign-On de la instancia de Platform Services Controller del partner. d Introduzca la contraseña del usuario administrador de vCenter Single Sign-On. e Haga clic en **Siguiente**. f Determine si desea crear un sitio de vCenter Single Sign-On o unirse a uno existente.

4 Revise la página del Programa de mejora de la experiencia del cliente (Customer Experience Improvement Program, CEIP) de VMware y decida si desea unirse a él.

Para obtener más información sobre el CEIP, consulte la sección Configurar el Programa de mejora de la experiencia del cliente en *Administrar vCenter Server y hosts*.

5 En la página Listo para finalizar, revise los ajustes de configuración del dispositivo de Platform Services Controller, haga clic en **Finalizar** y en **Aceptar** para completar la etapa 2 del proceso de implementación y configurar el dispositivo.

6 (opcional) Cuando termine la configuración inicial, haga clic en **https://*platform_services_controller_fqdn*/psc** para dirigirse a la interfaz web de Platform Services Controller o haga clic en **https://*platform_services_controller_fqdn*:443** para dirigirse a la página de introducción de Platform Services Controller.

7 Haga clic en **Cerrar** para cerrar el asistente.

   Se abrirá la página de introducción de Platform Services Controller.

Resultados

Si unió el nuevo dispositivo de Platform Services Controller a un dominio de vCenter Single Sign-On existente, el dispositivo replica los datos de infraestructura con las otras instancias de Platform Services Controller en el dominio.

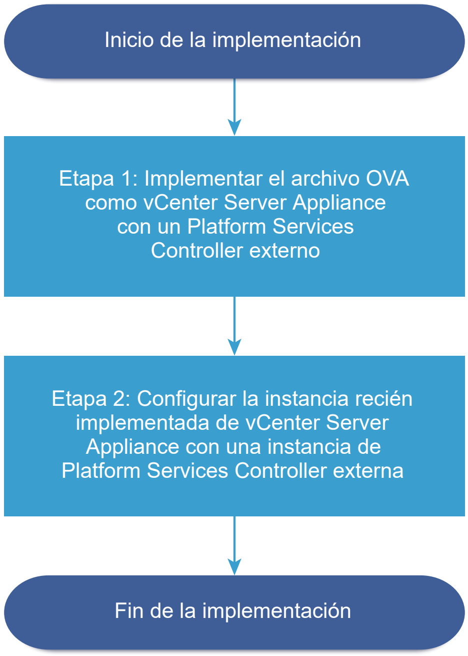
Pasos siguientes

- Puede implementar vCenter Server Appliance con una instancia de Platform Services Controller externa y registrarla con el dispositivo de Platform Services Controller recién implementado.
- Puede implementar una o más instancias de Platform Services Controller para que se unan al mismo dominio de vCenter Single Sign-On a fin de replicar los datos de infraestructura y distribuir la carga.

Implementar vCenter Server Appliance con una instancia de Platform Services Controller externa mediante la GUI

Puede utilizar el instalador de la GUI para realizar una implementación interactiva de una instancia de vCenter Server Appliance y registrarla con una instancia de Platform Services Controller externa. Se debe ejecutar la implementación de GUI desde un equipo Windows, Linux o Mac que se encuentre en la misma red en la que se desea implementar el dispositivo.

Figura 3-5. Implementación del flujo de trabajo de vCenter Server Appliance con una instancia externa de Platform Services Controller



Requisitos previos

- Consulte Requisitos previos para implementar vCenter Server Appliance o el dispositivo de Platform Services Controller.
- Consulte Información requerida para implementar una instancia de vCenter Server Appliance o un dispositivo de Platform Services Controller.
- Compruebe que ha instalado o implementado la instancia de Platform Services Controller con la que planea registrar vCenter Server Appliance.

Procedimiento

1 Etapa 1: Implementar el archivo OVA como vCenter Server Appliance con una instancia de Platform Services Controller externa

   En la etapa 1 del proceso de implementación se implementa el archivo OVA, incluido en el instalador de vCenter Server Appliance, como vCenter Server Appliance con una instancia de Platform Services Controller externa.

2 Etapa 2: Configurar el vCenter Server Appliance recién implementado con una instancia externa de Platform Services Controller

   Cuando finalice la implementación de OVA, se lo redirigirá a la etapa 2 del proceso de implementación para configurar e iniciar los servicios de vCenter Server Appliance recién implementado con una instancia externa de Platform Services Controller.

Etapa 1: Implementar el archivo OVA como vCenter Server Appliance con una instancia de Platform Services Controller externa

En la etapa 1 del proceso de implementación se implementa el archivo OVA, incluido en el instalador de vCenter Server Appliance, como vCenter Server Appliance con una instancia de Platform Services Controller externa.

Procedimiento

1. En el instalador de vCenter Server Appliance, desplácese hasta el directorio `vcsa-ui-installer`, vaya al subdirectorio del sistema operativo y ejecute el instalador.
   - En un sistema operativo Windows, vaya al subdirectorio `win32` y ejecute el archivo `installer.exe`.
   - En un sistema operativo Linux, vaya al subdirectorio `lin64` y ejecute el archivo `installer`.
   - En un sistema operativo Mac OS, vaya al subdirectorio `mac` y ejecute el archivo `Installer.app`.
2. En la página de inicio, haga clic en **Instalar** para iniciar el asistente de implementación.
3. Revise la página de introducción para comprender el proceso de implementación y haga clic en **Siguiente**.
4. Lea y acepte el contrato de licencia, y haga clic en **Siguiente**.
5. En la página Seleccionar tipo de implementación, seleccione **vCenter Server (requiere instancia externa de Platform Services Controller)** y haga clic en **Siguiente**.

6 Conéctese al servidor de destino donde desea implementar vCenter Server Appliance.

Opción	Pasos
Puede conectarse a un host ESXi para implementar el dispositivo allí.	1 Escriba el FQDN o la dirección IP del host ESXi. 2 Especifique el puerto HTTPS del host ESXi. 3 Escriba el nombre de usuario y la contraseña de un usuario que tenga privilegios administrativos en el host ESXi (por ejemplo, el usuario raíz). 4 Haga clic en **Siguiente**. 5 Asegúrese de que la advertencia de certificado muestre la huella digital SHA1 del certificado SSL que se instaló en el host ESXi de destino y haga clic en **Sí** para aceptar la huella digital del certificado.
Puede conectarse a una instancia de vCenter Server y examinar el inventario para seleccionar un host ESXi o un clúster de DRS donde se implementará el dispositivo.	1 Escriba el nombre de dominio completo o la dirección IP de la instancia de vCenter Server. 2 Especifique el puerto HTTPS de la instancia de vCenter Server. 3 Especifique el nombre de usuario y la contraseña de un usuario con privilegios administrativos de vCenter Single Sign-On en la instancia de vCenter Server (por ejemplo, el usuario administrator@*su_nombre_de_dominio*). 4 Haga clic en **Siguiente**. 5 Asegúrese de que la advertencia de certificado muestre la huella digital SHA1 del certificado SSL que se instaló en la instancia de vCenter Server de destino y haga clic en **Sí** para aceptar la huella digital del certificado. 6 Seleccione el centro de datos o la carpeta de centro de datos que contiene el host ESXi o el clúster de DRS donde desea implementar el dispositivo y haga clic en **Siguiente**. **Nota** Es necesario seleccionar un centro de datos o una carpeta de centro de datos que contenga al menos un host ESXi que no se encuentre en modo de bloqueo o de mantenimiento. 7 Seleccione el host ESXi o el clúster de DRS donde desea implementar el dispositivo y haga clic en **Siguiente**.

7 En la página Configurar máquina virtual de dispositivo, escriba un nombre para vCenter Server Appliance, establezca la contraseña del usuario raíz y haga clic en **Siguiente**.

El nombre del dispositivo no debe contener ningún signo de porcentaje (%), ninguna barra inversa (\) ni ninguna barra diagonal (/), y tampoco debe tener más de 80 caracteres.

La contraseña debe contener solo caracteres ASCII inferiores sin espacios, al menos ocho caracteres, un número, letras minúsculas y mayúsculas, y un carácter especial, por ejemplo, un signo de exclamación (!), un numeral (#), una arroba (@) o un paréntesis (()).

8 Seleccione el tamaño de la implementación para la instancia de vCenter Server Appliance de su inventario de vSphere.

Opción de tamaño de implementación	Descripción
Muy pequeño	Implementa un dispositivo con 2 CPU y 10 GB de memoria. Apropiado para entornos con hasta 10 hosts o 100 máquinas virtuales.
Pequeño	Implementa un dispositivo con 4 CPU y 16 GB de memoria. Apropiado para entornos con hasta 100 hosts o 1.000 máquinas virtuales.

Opción de tamaño de implementación	Descripción
Mediano	Implementa un dispositivo con 8 CPU y 24 GB de memoria. Apropiado para entornos con hasta 400 hosts o 4.000 máquinas virtuales.
Grande	Implementa un dispositivo con 16 CPU y 32 GB de memoria. Apropiado para entornos con hasta 1.000 hosts o 10.000 máquinas virtuales.
Extra grande	Implementa un dispositivo con 24 CPU y 48 GB de memoria. Apropiado para entornos con hasta 2.000 hosts o 35.000 máquinas virtuales.

9 Seleccione el tamaño de almacenamiento de vCenter Server Appliance y haga clic en **Siguiente**.

Opción de tamaño de almacenamiento	Descripción de tamaño de implementación muy pequeño	Descripción de tamaño de implementación pequeño	Descripción de tamaño de implementación mediano	Descripción de tamaño de implementación grande	Descripción de tamaño de implementación extragrande
Predeterminado	Implementa un dispositivo con 250 GB de almacenamiento.	Implementa un dispositivo con 290 GB de almacenamiento.	Implementa un dispositivo con 425 GB de almacenamiento.	Implementa un dispositivo con 640 GB de almacenamiento.	Implementa un dispositivo con 980 GB de almacenamiento.
Grande	Implementa un dispositivo con 775 GB de almacenamiento.	Implementa un dispositivo con 820 GB de almacenamiento.	Implementa un dispositivo con 925 GB de almacenamiento.	Implementa un dispositivo con 990 GB de almacenamiento.	Implementa un dispositivo con 1.030 GB de almacenamiento.
Extragrande	Implementa un dispositivo con 1.650 GB de almacenamiento.	Implementa un dispositivo con 1.700 GB de almacenamiento.	Implementa un dispositivo con 1.805 GB de almacenamiento.	Implementa un dispositivo con 1.870 GB de almacenamiento.	Implementa un dispositivo con 1.910 GB de almacenamiento.

10 En la lista de almacenes de datos disponibles, seleccione la ubicación en la que se almacenarán todos los archivos de configuración y discos virtuales de la máquina virtual. Opcionalmente, seleccione **Habilitar el modo de disco fino** para habilitar el aprovisionamiento fino.

11 En la página Ajustar la configuración de red, establezca la configuración de red.

La dirección IP o el FQDN del dispositivo se utilizan como nombre del sistema. Se recomienda utilizar un FQDN. Sin embargo, si desea utilizar una dirección IP, utilice asignación de direcciones IP estáticas del dispositivo, ya que las direcciones IP que asigna DHCP podrían cambiar.

Opción	Acción
Red	Seleccione la red a la que desea conectar el dispositivo. Las redes que se muestran en el menú desplegable dependen de la configuración de red del servidor de destino. En el caso de la implementación directa de un dispositivo en un host ESXi, los grupos de puertos virtuales distribuidos que no son efímeros no se admiten y no se muestran en el menú desplegable.
Versión IP	Seleccione la versión de la dirección IP del dispositivo. Puede seleccionar la versión IPv4 o IPv6.
Asignación de IP	Seleccione cómo asignar la dirección IP del dispositivo. ■ **estático** El asistente solicita que se introduzca la dirección IP y la configuración de red. **Nota** Evite utilizar una dirección IP como nombre del sistema. Si utiliza una dirección IP como nombre del sistema, no podrá cambiar la dirección IP ni actualizar la configuración de DNS después de la implementación; tampoco podrá unir el dispositivo a un dominio de Active Directory. ■ **DHCP** Los servidores DHCP se utilizan para asignar la dirección IP. Seleccione esta opción solo si hay un servidor DHCP disponible en el entorno. Si hay un DDNS habilitado en el entorno, puede escribir el nombre de dominio completo (Fully qualified domain name, FQDN) que prefiera para el dispositivo.
Puertos comunes	Puede personalizar los puertos HTTP y HTTPS (opcional). Si se especifican números de puerto HTTP y HTTPS personalizados, asegúrese de usar números de puerto que no se usen en vCenter Server, así como de evitar utilizar los puertos HTTP y HTTPS predeterminados (80 y 443). **Nota** Los puertos personalizados son compatibles a partir de vSphere 6.5 Update 2.

12 En la página Listo para finalizar la etapa 1, revise la configuración de implementación de vCenter Server Appliance y haga clic en **Finalizar** para iniciar el proceso de implementación de OVA.

13 Espere a que finalice la implementación de OVA y haga clic en **Continuar** para pasar a la etapa 2 del proceso de implementación a fin de configurar e iniciar los servicios del dispositivo recién implementado.

Nota Si hace clic en **Cerrar** para salir del asistente, deberá iniciar sesión en la interfaz de administración de vCenter Server Appliance para configurar e iniciar los servicios.

Resultados

La instancia de vCenter Server Appliance recién implementada con una instancia de Platform Services Controller externa se está ejecutando en el servidor de destino, pero los servicios no se han iniciado.

Etapa 2: Configurar el vCenter Server Appliance recién implementado con una instancia externa de Platform Services Controller

Cuando finalice la implementación de OVA, se lo redirigirá a la etapa 2 del proceso de implementación para configurar e iniciar los servicios de vCenter Server Appliance recién implementado con una instancia externa de Platform Services Controller.

Procedimiento

1 Revise la introducción a la etapa 2 del proceso de implementación y haga clic en **Siguiente**.

2 Ajuste la configuración de la hora en el dispositivo. De manera opcional, habilite el acceso SSH remoto al dispositivo y haga clic en **Siguiente**.

Opción	Descripción
Sincronizar la hora con el host ESXi	Habilita la sincronización horaria periódica y permite que VMware Tools establezca la hora del sistema operativo invitado para que sea la misma que la hora del host ESXi.
Sincronizar la hora con los servidores NTP	Utiliza un servidor de protocolo de tiempo de red para sincronizar la hora. Si selecciona esta opción, deberá escribir los nombres o las direcciones IP de los servidores NTP separados por comas.

3 Proporcione el FQDN o la dirección IP de la instancia de Platform Services Controller en la cual desea registrar vCenter Server Appliance, introduzca el puerto HTTPS de vCenter Single Sign-On, el nombre de dominio y la contraseña de administrador y, a continuación, haga clic en **Siguiente**.

Si la instancia de Platform Services Controller es una instalación de Windows, proporcione el nombre de sistema del equipo host en el cual se está ejecutando Platform Services Controller.

4 En la página Listo para finalizar, revise los ajustes de configuración de vCenter Server Appliance, y haga clic en **Finalizar** y en **Aceptar** para completar la etapa 2 del proceso de implementación y configurar el dispositivo.

5 (opcional) Cuando termine la configuración inicial, haga clic en **https://*vcenter_server_appliance_fqdn*/vsphere-client** para ir a vSphere Web Client e inicie sesión en la instancia de vCenter Server de vCenter Server Appliance, o bien haga clic en **https://*vcenter_server_appliance_fqdn*:443** para ir a la página de introducción de vCenter Server Appliance.

6 Haga clic en **Cerrar** para cerrar el asistente.

   Se abrirá la página de introducción de vCenter Server Appliance.

Resultados

La instancia de vCenter Server Appliance recién implementada se unió al dominio de vCenter Single Sign-On y al sitio de la instancia de Platform Services Controller en la cual se registró el dispositivo.

Pasos siguientes

Es posible configurar la alta disponibilidad para vCenter Server Appliance. Para obtener información sobre la forma de proporcionar alta disponibilidad a vCenter Server Appliance, consulte *Disponibilidad de vSphere*.

Implementación de CLI en vCenter Server Appliance y en el dispositivo de Platform Services Controller

Puede utilizar el instalador de CLI para realizar la implementación silenciosa de vCenter Server Appliance o un dispositivo de Platform Services Controller en un host ESXi o una instancia de vCenter Server.

El proceso de implementación de CLI incluye: descargar el instalador de vCenter Server Appliance en la máquina virtual de red o en el servidor físico desde donde se desea realizar la implementación; preparar un archivo de configuración JSON con la información de implementación; y ejecutar el comando de implementación.

Importante El nombre de usuario que utilizará para iniciar sesión en la máquina desde donde desea ejecutar el instalador de CLI, la ruta de acceso al instalador de vCenter Server Appliance, la ruta de acceso al archivo de configuración JSON y sus valores de cadena, incluidas las contraseñas, deben contener solamente caracteres ASCII. No se admiten los caracteres ASCII extendidos ni los caracteres que no sean ASCII.

El archivo ISO de vCenter Server Appliance contiene plantillas de los archivos JSON que incluyen los parámetros mínimos de configuración requeridos para implementar vCenter Server Appliance o un dispositivo de Platform Services Controller.

El archivo ISO de vCenter Server Appliance contiene plantillas de los archivos JSON que incluyen los parámetros mínimos de configuración requeridos para implementar vCenter Server Appliance o un dispositivo de Platform Services Controller. Para obtener información sobre la preparación de plantillas JSON para la implementación de CLI, consulte Preparar el archivo de configuración JSON para la implementación de CLI.

Importante Para usar topologías con instancias externas de Platform Services Controller, es necesario implementar las instancias de replicación de Platform Services Controller en secuencia. Después de implementar correctamente todas las instancias de Platform Services Controller en el dominio, se pueden realizar implementaciones simultáneas de varios dispositivos de vCenter Server que apuntan a una instancia externa común de Platform Services Controller.

Preparar el archivo de configuración JSON para la implementación de CLI

Antes de ejecutar el instalador CLI para implementar una instancia de vCenter Server Appliance o un dispositivo de Platform Services Controller, debe preparar un archivo JSON con los parámetros de configuración y sus valores para la especificación de la implementación.

El instalador de vCenter Server Appliance contiene plantillas JSON para todos los tipos de implementación. Para obtener información sobre las plantillas, consulte Plantillas JSON para la implementación de CLI de vCenter Server Appliance y del dispositivo de Platform Services Controller.

Para implementar un dispositivo con la configuración mínima, establezca los valores según los parámetros de configuración en la plantilla JSON correspondiente a su especificación. Puede editar los valores preestablecidos, quitar los parámetros de configuración y agregar parámetros para configuraciones personalizadas.

Si desea conocer la lista completa de parámetros de configuración y sus descripciones, desplácese hasta el subdirectorio del instalador del sistema operativo y ejecute el comando `vcsa-deploy install --template-help`, o bien consulte Parámetros de configuración de implementación.

Requisitos previos

- Debe estar familiarizado con la sintaxis JSON.
- Descargar y montar el instalador de vCenter Server Appliance.

Procedimiento

1 En el instalador de vCenter Server Appliance, desplácese hasta el directorio `vcsa-cli-installer` y abra la subcarpeta `plantillas`.

2 Copie las plantillas de implementación desde la subcarpeta `install` en su área de trabajo.

Importante La ruta de acceso a los archivos de configuración JSON debe contener únicamente caracteres ASCII. No se admiten los caracteres ASCII extendidos ni los caracteres que no sean ASCII.

3 En un editor de texto, abra el archivo de plantilla de la especificación.

Para garantizar la correcta sintaxis del archivo de configuración JSON, use un editor JSON.

4 Complete los valores para los parámetros de configuración requeridos y, como opción, introduzca parámetros adicionales y sus valores.

Por ejemplo, si desea utilizar una asignación de DHCP IPv4 para la red del dispositivo, en la subsección `network` de la plantilla, cambie el valor del parámetro `mode` a `dhcp` y quite los parámetros de configuración predeterminados que son para una asignación estática.

```
        "network": {
            "ip.family": "ipv4",
            "mode": "dhcp"
        },
```

Importante Los valores de cadena, incluidas las contraseñas, deben contener únicamente caracteres ASCII. No se admiten los caracteres ASCII extendidos ni los caracteres que no sean ASCII.

Para establecer un valor que contiene una barra diagonal inversa (\) o un carácter de comillas ("), debe anteponer a este carácter una barra diagonal inversa (\). Por ejemplo, `"password":"my\"password"` establece la contraseña my"password y `"image":"G:\\vcsa\\VMware-vCenter-Server-Appliance-6.5.0.`*`XXXX`*`-`*`YYYYYYY`*`_OVF10.ova"` establece la ruta de acceso `G:\vcsa\VMware-vCenter-Server-Appliance-6.5.0.`*`XXXX`*`-`*`YYYYYYY`*`_OVF10.ova`.

Los valores booleanos deben contener únicamente caracteres en minúsculas; es decir, un valor puede ser `true` o `false`. Por ejemplo, `"ssh.enable":false`.

5 (opcional) Para validar un archivo JSON, utilice un editor JSON de su elección.

6 Guárdelo en formato UTF-8 y cierre el archivo.

Pasos siguientes

Puede crear y guardar plantillas adicionales, si fuera necesario, para la especificación de la implementación.

Plantillas JSON para la implementación de CLI de vCenter Server Appliance y del dispositivo de Platform Services Controller

El instalador de vCenter Server Appliance contiene plantillas JSON que están ubicadas en el directorio `vcsa-cli-installer/templates`. En la subcarpeta `install`, se pueden encontrar

ocho plantillas JSON con los parámetros de configuración mínimos para todos los tipos de implementación.

Por cada tipo de implementación, hay una plantilla que permite implementar el dispositivo en un host ESXiy otra plantilla que permite implementar el dispositivo en una instancia de vCenter Server.

Tabla 3-7. Las plantillas de implementación JSON se incluyen en el instalador de vCenter Server Appliance.

Ubicación	Plantilla	Descripción
`vcsa-cli-installer\templates\install`	`embedded_vCSA_on_ESXi.json`	Contiene los parámetros de configuración mínimos que son obligatorios para la implementación de vCenter Server Appliancecon una instancia integrada de Platform Services Controller en un host ESXi.
	`embedded_vCSA_on_VC.json`	Contiene los parámetros de configuración mínimos que son obligatorios para la implementación de vCenter Server Appliancecon una instancia integrada de Platform Services Controller en una instancia de vCenter Server.
	`embedded_vCSA_replication_on_ESXi.json`	Contiene los parámetros de configuración mínimos que son obligatorios para la implementación de una instancia de vCenter Server Appliance con una instancia integrada de Platform Services Controller como un partner de replicación en otra instancia integrada de vCenter Server Appliance en un host ESXi.
	`embedded_vCSA_replication_on_VC.json`	Contiene los parámetros de configuración mínimos que son obligatorios para la implementación de una instancia de vCenter Server Appliance con una instancia integrada de Platform Services Controller como un partner de replicación en otra instancia integrada de vCenter Server Appliance en una instancia de vCenter Server.
	`PSC_first_instance_on_ESXi.json`	Contiene los parámetros de configuración mínimos que son obligatorios para la implementación de un dispositivo de Platform Services Controller como primera instancia en nuevo dominio de vCenter Single Sign-On en un host ESXi.

Tabla 3-7. Las plantillas de implementación JSON se incluyen en el instalador de vCenter Server Appliance. (continuación)

Ubicación	Plantilla	Descripción
	`PSC_first_instance_on_VC.json`	Contiene los parámetros de configuración mínimos que son obligatorios para la implementación de un dispositivo de Platform Services Controller como primera instancia en un nuevo dominio de vCenter Single Sign-On en una instancia de vCenter Server.
	`PSC_replication_on_ESXi.json`	Contiene los parámetros de configuración mínimos que son obligatorios para la implementación de un dispositivo de Platform Services Controller que se une a un dominio existente de vCenter Single Sign-On en un host ESXi.
	`PSC_replication_on_VC.json`	Contiene los parámetros de configuración mínimos que son obligatorios para la implementación de un dispositivo de Platform Services Controller que se une a un dominio existente de vCenter Single Sign-On en una instancia de vCenter Server.
	`vCSA_on_ESXi.json`	Contiene los parámetros de configuración mínimos que son obligatorios para la implementación de vCenter Server Appliancecon una instancia externa de Platform Services Controller en un host ESXi.
	`vCSA_on_VC.json`	Contiene los parámetros de configuración mínimos que son obligatorios para la implementación de vCenter Server Appliancecon una instancia externa de Platform Services Controller en una instancia de vCenter Server.

Parámetros de configuración de implementación

Cuando se preparan los archivos de configuración JSON para la implementación de CLI, es necesario establecer parámetros y valores con el fin de proporcionar los datos de entrada para la implementación de vCenter Server Appliance o un dispositivo de Platform Services Controller.

Secciones y subsecciones de los parámetros de configuración en los archivos de implementación JSON

Los parámetros de configuración en los archivos de configuración JSON para la actualización de CLI se organizan en secciones y subsecciones.

Tabla 3-8. Secciones y subsecciones de los parámetros de configuración en los archivos de implementación JSON

Sección	Subsección	Descripción
`new.vcsa`: describe el dispositivo que se desea implementar.	`esxi`	Se utiliza únicamente si se desea implementar el dispositivo directamente en un host ESXi. Contiene los parámetros de configuración que describen el host ESXi de destino. Consulte Tabla 3-9. Parámetros de configuración en la sección new.vcsa, subsección esxi. **Nota** Es necesario completar la subsección `esxi` o `vc`.
	`vc`	Se utiliza únicamente si se desea implementar el dispositivo en el inventario de una instancia de vCenter Server. Se incluyen los parámetros de configuración que describen el host ESXi o el clúster de DRS de destino del inventario de vCenter Server. Consulte Tabla 3-10. Parámetros de configuración en la sección new.vcsa, subsección vc. **Nota** Es necesario completar la subsección `vc` o `esxi`.
	`appliance`	Se incluyen los parámetros de configuración que describen el dispositivo. Consulte Tabla 3-11. Parámetros de configuración en la sección new.vcsa, subsección appliance.
	`network`	Se incluyen los parámetros de configuración que describen la configuración de red del dispositivo. Consulte Tabla 3-12. Parámetros de configuración en la sección new.vcsa, subsección network.
	`os`	Se incluyen los parámetros de configuración que describen la configuración del sistema operativo del dispositivo. Consulte Tabla 3-13. Parámetros de configuración en la sección new.vcsa, subsección os.
	`sso`	Se incluyen los parámetros de configuración que describen la configuración de vCenter Single Sign-On para el dispositivo. Consulte Tabla 3-14. Parámetros de configuración en la sección new.vcsa, subsección sso.

Tabla 3-8. Secciones y subsecciones de los parámetros de configuración en los archivos de implementación JSON (continuación)

Sección	Subsección	Descripción
	`ovftool.arguments`	Subsección opcional para agregar argumentos arbitrarios y sus valores al comando de OVF Tool generado por el instalador. **Importante** El instalador de vCenter Server Appliance no valida los parámetros de configuración de la subsección `ovftool.arguments`. Si se establecen argumentos que OVF Tool no reconoce, es posible que se produzcan errores en la implementación.
`ceip`: describe la unión al programa de mejora de la experiencia de cliente (Customer Experience Improvement Program, CEIP) de VMware.	`settings`	Se incluye solamente el parámetro de configuración `ceip.enabled` para unirse o no unirse al programa de mejora de la experiencia de cliente (Customer Experience Improvement Program, CEIP) de VMware. Consulte Tabla 3-15. Parámetros de configuración en la sección ceip, subsección settings. Solo es necesario si se realiza una implementación de vCenter Server Appliance con una instancia integrada de Platform Services Controller o un dispositivo de Platform Services Controller. **Nota** Si se establece en `true`, se debe ejecutar el comando de implementación de CLI con el argumento `--acknowledge-ceip`. Para obtener más información sobre el CEIP, consulte la sección Configurar el Programa de mejora de la experiencia del cliente en *Administrar vCenter Server y hosts*.

Importante Los valores de cadena, incluidas las contraseñas, deben contener únicamente caracteres ASCII. No se admiten los caracteres ASCII extendidos ni los caracteres que no sean ASCII.

Para establecer un valor que contiene una barra diagonal inversa (\) o un carácter de comillas ("), debe anteponer a este carácter una barra diagonal inversa (\). Por ejemplo, `"password":"my\"password"` establece la contraseña my"password y `"image":"G:\\vcsa\\VMware-vCenter-Server-Appliance-6.5.0.`*`XXXX-YYYYYYY`*`_OVF10.ova"` establece la ruta de acceso `G:\vcsa\VMware-vCenter-Server-Appliance-6.5.0.`*`XXXX-YYYYYYY`*`_OVF10.ova`.

Los valores booleanos solo deben contener caracteres en minúscula. Pueden ser `true` o `false`. Por ejemplo, `"ssh.enable":false`.

Parámetros de configuración en la sección `new.vcsa`

Tabla 3-9. Parámetros de configuración en la sección `new.vcsa`, subsección `esxi`

Nombre	Tipo	Descripción
`hostname`	string	La dirección IP o el FQDN del host ESXi de destino en el que se desea implementar el dispositivo.
`username`	string	Un nombre de usuario con privilegios administrativos en el host ESXi de destino (por ejemplo, raíz).
`password`	string	La contraseña del usuario con privilegios administrativos en el host ESXi de destino.

Tabla 3-9. Parámetros de configuración en la sección `new.vcsa`, subsección `esxi` (continuación)

Nombre	Tipo	Descripción
`deployment.network`	string	El nombre de la red a la que se conectará el dispositivo. **Nota** El acceso a la red debe ser posible desde el host ESXi de destino. Se omite si el host ESXi de destino tiene una sola red.
`datastore`	string	El nombre del almacén de datos en el que se almacenarán todos los archivos de configuración de las máquinas virtuales y los discos virtuales del dispositivo. **Nota** Debe ser posible acceder al almacén de datos desde el host ESXi. El almacén de datos debe tener suficiente espacio libre.
`port`	entero	El puerto de proxy inverso HTTPS del host ESXi de destino. El puerto predeterminado es 443. Se utiliza únicamente si el host ESXi de destino usa un puerto de proxy inverso HTTPS personalizado.

Tabla 3-10. Parámetros de configuración en la sección `new.vcsa`, subsección `vc`

Nombre	Tipo	Descripción
`hostname`	string	La dirección IP o el FQDN de la instancia de vCenter Server de destino en el que se desea implementar el dispositivo.
`username`	string	El nombre del usuario administrador de vCenter Single Sign-On en la instancia de vCenter Server de destino, por ejemplo, administrator@vsphere.local.
`password`	string	La contraseña del usuario administrador de vCenter Single Sign-On en la instancia de vCenter Server de destino.
`deployment.network`	string	El nombre de la red a la que se conectará el dispositivo. **Nota** Debe ser posible acceder a la red desde el host ESXi o el clúster de DRS de destino en el que se desea implementar el dispositivo. Se omite si el host ESXi o el clúster de DRS de destino tienen una sola red.

`datacenter`	cadena o matriz	El centro de datos de vCenter Server que contiene el host ESXi o el clúster de DRS de destino en el que se desea implementar el dispositivo.
		Si el centro de datos se encuentra en una carpeta o una estructura de carpetas, el valor debe ser una lista de cadenas separada por comas o una lista separada por comas como una sola cadena. Por ejemplo,
		`["parent_folder", "child_folder", "datacenter_name"]`
		o
		`"parent_folder, child_folder, datacenter_name"`
		Nota El valor distingue entre mayúsculas y minúsculas.

`datastore`	string	El nombre del almacén de datos en el que se almacenarán todos los archivos de configuración de las máquinas virtuales y los discos virtuales del dispositivo. **Nota** El acceso al almacén de datos debe ser posible desde el host ESXi o el clúster de DRS de destino. El almacén de datos debe tener al menos 15 GB de espacio libre.

Tabla 3-10. Parámetros de configuración en la sección `new.vcsa`, subsección `vc` (continuación)

Nombre	Tipo	Descripción
`port`	entero	El puerto de proxy inverso HTTPS de la instancia de vCenter Server de destino. El puerto predeterminado es 443. Se utiliza únicamente si la instancia de vCenter Server de destino usa un puerto de proxy inverso HTTPS personalizado.

`target`	cadena o matriz	El host ESXi o el clúster de DRS de destino en el que se desea implementar el dispositivo.
		Importante Es necesario proporcionar el nombre que se muestra en el inventario de vCenter Server. Por ejemplo, si el nombre del host ESXi de destino es una dirección IP en el inventario de vCenter Server, no se puede proporcionar un FQDN.
		Si el host ESXi o el clúster de DRS de destino se encuentran en una carpeta o una estructura de carpetas, el valor debe ser una lista de cadenas separada por comas o una lista separada por comas como una sola cadena. Por ejemplo,
		`["parent_folder", "child_folder", "esxi-host.domain.com"]`
		o
		`"parent_folder, child_folder, esxi-host.domain.com"`
		Si el host ESXi de destino forma parte de un clúster, utilice una lista de cadenas separada por comas o una lista separada por comas como una sola cadena para proporcionar la ruta de acceso. Por ejemplo,
		`["cluster_name", "esxi-host.domain.com"]`
		o
		`"cluster_name, esxi-host.domain.com"`
		Nota El valor distingue entre mayúsculas y minúsculas.

`vm.folder`	string	Opcional. El nombre de la carpeta de máquina virtual a la que se agregará el dispositivo.

Tabla 3-11. Parámetros de configuración en la sección `new.vcsa`, subsección `appliance`

Nombre	Tipo	Descripción
`thin.disk.mode`	Booleano	Se establece en `true` para implementar el dispositivo con discos virtuales finos.
`deployment.option`	string	El tamaño del dispositivo. ■ Se establece en `tiny` si se desea implementar un dispositivo de vCenter Server Appliance con una instancia integrada de Platform Services Controller para hasta 10 hosts y 100 máquinas virtuales con el tamaño de almacenamiento predeterminado. Se implementa un dispositivo con 2 CPU, 10 GB de memoria y 250 GB de almacenamiento. ■ Se establece en `tiny-lstorage` si se desea implementar un dispositivo de vCenter Server Appliance con una instancia integrada de Platform Services Controller para hasta 10 hosts y 100 máquinas virtuales con el tamaño de almacenamiento grande. Se implementa un dispositivo con 2 CPU, 10 GB de memoria y 775 GB de almacenamiento. ■ Se establece en `tiny-xlstorage` si se desea implementar un dispositivo de vCenter Server Appliance con una instancia integrada de Platform Services Controller para hasta 10 hosts y 100 máquinas virtuales con el tamaño de almacenamiento extragrande. Se implementa un dispositivo con 2 CPU, 10 GB de memoria y 1.650 GB de almacenamiento. ■ Se establece en `small` si se desea implementar un dispositivo de vCenter Server Appliance con una instancia integrada de Platform Services Controller para hasta 100 hosts y 1.000 máquinas virtuales con el tamaño de almacenamiento predeterminado. Se implementa un dispositivo con 4 CPU, 16 GB de memoria y 290 GB de almacenamiento. ■ Se establece en `small-lstorage` si se desea implementar un dispositivo de vCenter Server Appliance con una instancia integrada de Platform Services Controller para hasta 100 hosts y 1.000 máquinas virtuales con el tamaño de almacenamiento grande. Se implementa un dispositivo con 4 CPU, 16 GB de memoria y 820 GB de almacenamiento. ■ Se establece en `small-xlstorage` si se desea implementar un dispositivo de vCenter Server Appliance con una instancia integrada de Platform Services Controller para hasta 100 hosts y 1.000 máquinas virtuales con el tamaño de almacenamiento extragrande. Se implementa un dispositivo con 4 CPU, 16 GB de memoria y 1.700 GB de almacenamiento. ■ Se establece en `medium` si se desea implementar un dispositivo de vCenter Server Appliance con una instancia integrada de Platform Services Controller para hasta 400 hosts y 4.000 máquinas virtuales con el tamaño de almacenamiento predeterminado. Se implementa un dispositivo con 8 CPU, 24 GB de memoria y 425 GB de almacenamiento.

Tabla 3-11. Parámetros de configuración en la sección `new.vcsa`, subsección `appliance` (continuación)

Nombre	Tipo	Descripción
		■ Se establece en `medium-lstorage` si se desea implementar un dispositivo de vCenter Server Appliance con una instancia integrada de Platform Services Controller para hasta 400 hosts y 4.000 máquinas virtuales con el tamaño de almacenamiento grande. Se implementa un dispositivo con 8 CPU, 24 GB de memoria y 925 GB de almacenamiento. ■ Se establece en `medium-xlstorage` si se desea implementar un dispositivo de vCenter Server Appliance con una instancia integrada de Platform Services Controller para hasta 400 hosts y 4.000 máquinas virtuales con el tamaño de almacenamiento extragrande. Se implementa un dispositivo con 8 CPU, 24 GB de memoria y 1.805 GB de almacenamiento. ■ Se establece en `large` si se desea implementar un dispositivo de vCenter Server Appliance con una instancia integrada de Platform Services Controller para hasta 1.000 hosts y 10.000 máquinas virtuales con el tamaño de almacenamiento predeterminado. Se implementa un dispositivo con 16 CPU, 32 GB de memoria y 640 GB de almacenamiento. ■ Se establece en `large-lstorage` si se desea implementar un dispositivo de vCenter Server Appliance con una instancia integrada de Platform Services Controller para hasta 1.000 hosts y 10.000 máquinas virtuales con el tamaño de almacenamiento grande. Se implementa un dispositivo con 16 CPU, 32 GB de memoria y 990 GB de almacenamiento. ■ Se establece en `large-xlstorage` si se desea implementar un dispositivo de vCenter Server Appliance con una instancia integrada de Platform Services Controller para hasta 1.000 hosts y 10.000 máquinas virtuales con el tamaño de almacenamiento extragrande. Se implementa un dispositivo con 16 CPU, 32 GB de memoria y 1.870 GB de almacenamiento. ■ Se establece en `xlarge` si se desea implementar un dispositivo de vCenter Server Appliance con una instancia integrada de Platform Services Controller para hasta 2.000 hosts y 35.000 máquinas virtuales con el tamaño de almacenamiento predeterminado. Se implementa un dispositivo con 24 CPU, 48 GB de memoria y 980 GB de almacenamiento. ■ Se establece en `xlarge-lstorage` si se desea implementar un dispositivo de vCenter Server Appliance con una instancia integrada de Platform Services Controller para hasta 2.000 hosts y 35.000 máquinas virtuales con el tamaño de almacenamiento grande. Se implementa un dispositivo con 24 CPU, 48 GB de memoria y 1.030 GB de almacenamiento.

Tabla 3-11. Parámetros de configuración en la sección `new.vcsa`, subsección `appliance` (continuación)

Nombre	Tipo	Descripción
		■ Se establece en `xlarge-xlstorage` si se desea implementar un dispositivo de vCenter Server Appliance con una instancia integrada de Platform Services Controller para hasta 2.000 hosts y 35.000 máquinas virtuales con el tamaño de almacenamiento extragrande. Se implementa un dispositivo con 24 CPU, 48 GB de memoria y 1.910 GB de almacenamiento. ■ Se establece en `management-tiny` si se desea implementar un dispositivo de vCenter Server Appliance con una instancia externa de Platform Services Controller para hasta 10 hosts y 100 máquinas virtuales con el tamaño de almacenamiento predeterminado. Se implementa un dispositivo con 2 CPU, 10 GB de memoria y 250 GB de almacenamiento. ■ Se establece en `management-tiny-lstorage` si se desea implementar un dispositivo de vCenter Server Appliance con una instancia externa de Platform Services Controller para hasta 10 hosts y 100 máquinas virtuales con el tamaño de almacenamiento grande. Se implementa un dispositivo con 2 CPU, 10 GB de memoria y 775 GB de almacenamiento. ■ Se establece en `management-tiny-xlstorage` si se desea implementar un dispositivo de vCenter Server Appliance con una instancia externa de Platform Services Controller para hasta 10 hosts y 100 máquinas virtuales con el tamaño de almacenamiento extragrande. Se implementa un dispositivo con 2 CPU, 10 GB de memoria y 1.650 GB de almacenamiento. ■ Se establece en `management-small` si se desea implementar un dispositivo de vCenter Server Appliance con una instancia externa de Platform Services Controller para hasta 100 hosts y 1.000 máquinas virtuales con el tamaño de almacenamiento predeterminado. Se implementa un dispositivo con 4 CPU, 16 GB de memoria y 290 GB de almacenamiento. ■ Se establece en `management-small-lstorage` si se desea implementar un dispositivo de vCenter Server Appliance con una instancia externa de Platform Services Controller para hasta 100 hosts y 1.000 máquinas virtuales con el tamaño de almacenamiento grande. Se implementa un dispositivo con 4 CPU, 16 GB de memoria y 820 GB de almacenamiento. ■ Se establece en `management-small-xlstorage` si se desea implementar un dispositivo de vCenter Server Appliance con una instancia externa de Platform Services Controller para hasta 100 hosts y 1.000 máquinas virtuales con el tamaño de almacenamiento extragrande. Se implementa un dispositivo con 4 CPU, 16 GB de memoria y 1.700 GB de almacenamiento.

Tabla 3-11. Parámetros de configuración en la sección `new.vcsa`, subsección `appliance` (continuación)

Nombre	Tipo	Descripción
		■ Se establece en `management-medium` si se desea implementar un dispositivo de vCenter Server Appliance con una instancia externa de Platform Services Controller para hasta 400 hosts y 4.000 máquinas virtuales con el tamaño de almacenamiento predeterminado. Se implementa un dispositivo con 8 CPU, 24 GB de memoria y 425 GB de almacenamiento. ■ Se establece en `management-medium-lstorage` si se desea implementar un dispositivo de vCenter Server Appliance con una instancia externa de Platform Services Controller para hasta 400 hosts y 4.000 máquinas virtuales con el tamaño de almacenamiento grande. Se implementa un dispositivo con 8 CPU, 24 GB de memoria y 925 GB de almacenamiento. ■ Se establece en `management-medium-xlstorage` si se desea implementar un dispositivo de vCenter Server Appliance con una instancia externa de Platform Services Controller para hasta 400 hosts y 4.000 máquinas virtuales con el tamaño de almacenamiento extragrande. Se implementa un dispositivo con 8 CPU, 24 GB de memoria y 1.805 GB de almacenamiento. ■ Se establece en `management-large` si se desea implementar un dispositivo de vCenter Server Appliance con una instancia externa de Platform Services Controller para hasta 1.000 hosts y 10.000 máquinas virtuales con el tamaño de almacenamiento predeterminado. Se implementa un dispositivo con 16 CPU, 32 GB de memoria y 640 GB de almacenamiento. ■ Se establece en `management-large-lstorage` si se desea implementar un dispositivo de vCenter Server Appliance con una instancia externa de Platform Services Controller para hasta 1.000 hosts y 10.000 máquinas virtuales con el tamaño de almacenamiento grande. Se implementa un dispositivo con 16 CPU, 32 GB de memoria y 990 GB de almacenamiento. ■ Se establece en `management-large-xlstorage` si se desea implementar un dispositivo de vCenter Server Appliance con una instancia externa de Platform Services Controller para hasta 1.000 hosts y 10.000 máquinas virtuales con el tamaño de almacenamiento extragrande. Se implementa un dispositivo con 16 CPU, 32 GB de memoria y 1.870 GB de almacenamiento. ■ Se establece en `management-xlarge` si se desea implementar un dispositivo de vCenter Server Appliance con una instancia externa de Platform Services Controller para hasta 2.000 hosts y 35.000 máquinas virtuales con el tamaño de almacenamiento predeterminado. Se implementa un dispositivo con 24 CPU, 48 GB de memoria y 980 GB de almacenamiento.

Tabla 3-11. Parámetros de configuración en la sección `new.vcsa`, subsección `appliance` (continuación)

Nombre	Tipo	Descripción
		■ Se establece en `management-xlarge-lstorage` si se desea implementar un dispositivo de vCenter Server Appliance con una instancia externa de Platform Services Controller para hasta 2.000 hosts y 35.000 máquinas virtuales con el tamaño de almacenamiento grande. Se implementa un dispositivo con 24 CPU, 48 GB de memoria y 1.030 GB de almacenamiento. ■ Se establece en `management-xlarge-xlstorage` si se desea implementar un dispositivo de vCenter Server Appliance con una instancia externa de Platform Services Controller para hasta 2.000 hosts y 35.000 máquinas virtuales con el tamaño de almacenamiento extragrande. Se implementa un dispositivo con 24 CPU, 48 GB de memoria y 1.910 GB de almacenamiento. ■ Se establece en `infrastructure` si se desea implementar un dispositivo de Platform Services Controller. Se implementa un dispositivo con 2 CPU, 4 GB de memoria y 60 GB de almacenamiento.
`image`	string	Opcional. Una dirección URL o una ruta de acceso de archivo local al paquete de instalación de vCenter Server Appliance. De forma predeterminada, el instalador utiliza el paquete de instalación que se incluye en el archivo ISO de la carpeta `vcsa`.
`name`	string	El nombre de la máquina virtual para el dispositivo. Solo se deben incluir caracteres ASCII, excepto el signo de porcentaje (%), la barra diagonal inversa (\) o la barra diagonal (/), y no se deben superar los 80 caracteres de longitud.
`ovftool.path`	string	Opcional. Una ruta de acceso de archivo local al archivo ejecutable de OVF Tool. De forma predeterminada, el instalador utiliza la instancia de OVF Tool que se incluye en el archivo ISO de la carpeta `vcsa/ovftool`.

Tabla 3-12. Parámetros de configuración en la sección `new.vcsa`, subsección `network`

Nombre	Tipo	Descripción
`ip.family`	string	La versión de IP para la red del dispositivo. Se establece en `ipv4` o `ipv6`.
`mode`	string	La asignación de IP para la red del dispositivo. Se establece en `static` o `dhcp`.
`ip`	string	La dirección IP del dispositivo. Solo se requiere si se utiliza una asignación estática, es decir, si se establece el parámetro `mode` en `static`. Es necesario establecer una dirección IPv4 o IPv6 que coincida con la versión de IP de la red, es decir, con el valor del parámetro `ip.family`. Una dirección IPv4 debe cumplir con las directrices RFC 790. Una dirección IPv6 debe cumplir con las directrices RFC 2373.

Tabla 3-12. Parámetros de configuración en la sección `new.vcsa`, subsección `network` (continuación)

Nombre	Tipo	Descripción

`dns.servers`	cadena o matriz	Direcciones IP de uno o varios servidores DNS.
		Para establecer más de un servidor DNS, utilice una lista de cadenas separada por comas o una lista separada por comas como una sola cadena para proporcionar la ruta de acceso. Por ejemplo,
		`["x.y.z.a", "x.y.z.b"]`
		o
		`"x.y.z.a, x.y.z.b"`
		Solo se requiere si se utiliza una asignación estática, es decir, si se establece el parámetro `mode` en `static`.

`prefix`	string	Longitud del prefijo de red. Usar solo si el parámetro `mode` se establece en `static`. Eliminar si el parámetro `mode` se establece en `dhcp`. La longitud del prefijo de red es el número de bits que se establecen en la máscara de subred. Por ejemplo, si la máscara de subred es 255.255.255.0, hay 24 bits en la versión binaria de la longitud del prefijo, por lo que la longitud del prefijo de red es 24. Para la versión de IPv4, el valor debe estar entre `0` y `32`. Para la versión de IPv6, el valor debe estar entre `0` y `128`.
`gateway`	string	Dirección IP de la puerta de enlace predeterminada. Para la versión de IPv6, el valor puede ser `default`.

Tabla 3-12. Parámetros de configuración en la sección `new.vcsa`, subsección `network` (continuación)

Nombre	Tipo	Descripción

`ports`	string	(Opcional) Números de puerto que vCenter Server Appliance utiliza para las conexiones HTTP directas. De forma predeterminada, el puerto 80 redirecciona las solicitudes al puerto HTTPS 443. Puede personalizar los puertos HTTP y HTTPS de vCenter Server. Si desea especificar un número de puerto HTTP y HTTPS personalizado, asegúrese de no usar un puerto que ya se use en vCenter Server ni los puertos HTTP y HTTPS 80 y 443 predeterminados.
		Las opciones para especificar un puerto personalizado son: `"rhttpproxy.ext.port1":"`*`número_puerto`*`"` para el puerto HTTP y `"rhttpproxy.ext.port2:"`*`número_puerto`*`"` para el puerto HTTPS.
		El siguiente ejemplo especifica los puertos 81 y 444 para los puertos HTTP y HTTPS:
		`ports: {"rhttpproxy.ext.port1":"81",`
		`"rhttpproxy.ext.port2":"444"}`
		Para obtener más información sobre los puertos utilizados en vCenter Server, consulte Puertos necesarios para vCenter Server y Platform Services Controller.
		Nota El parámetro `ports` se admite a partir de vSphere 6.5 Update 2.

`system.name`	string	Identidad de red principal. Puede ser una dirección IP o un FQDN (de preferencia, FQDN). No se puede cambiar el valor de este parámetro después de la implementación. El FQDN y los números con punto decimal deben cumplir con las directrices RFC 1123.

Tabla 3-13. Parámetros de configuración en la sección `new.vcsa`, subsección `os`

Nombre	Tipo	Descripción
`password`	string	La contraseña del usuario raíz del sistema operativo del dispositivo. La contraseña debe tener entre 8 y 20 caracteres, y debe contener al menos uno de los siguientes tipos de carácter: una mayúscula, una minúscula, un número y un carácter especial, como por ejemplo, un signo de dólar ($), un numeral (#), una arroba (@), un punto (.) o un signo de exclamación (!). Todos los caracteres deben ser caracteres ASCII inferiores sin espacios.

`ntp.servers`	cadena o matriz	Opcional. Nombres de host o direcciones IP de uno o varios servidores NTP para la sincronización de hora.
		Para establecer más de un servidor NTP, utilice una lista de cadenas separada por comas o una lista separada por comas como una sola cadena para proporcionar la ruta de acceso. Por ejemplo,
		`["x.y.z.a", "x.y.z.b"]`
		o
		`"x.y.z.a, x.y.z.b"`

Tabla 3-13. Parámetros de configuración en la sección `new.vcsa`, subsección `os` (continuación)

Nombre	Tipo	Descripción
`ssh.enable`	Booleano	Se establece en `true` para habilitar el inicio de sesión del administrador de SSH en el dispositivo. **Nota** vCenter Server Appliance de alta disponibilidad requiere acceso SSH remoto al dispositivo.
`time.tools-sync`	Booleano	Opcional. Se establece en `true` para implementar el dispositivo con la sincronización de hora de VMware Tools. VMware Tools sincroniza la hora del dispositivo con la hora del host ESXi. Se omite si los servidores NTP se establecen para la sincronización de hora; es decir, si se establece el parámetro `ntp.servers`.

Tabla 3-14. Parámetros de configuración en la sección `new.vcsa`, subsección `sso`

Nombre	Tipo	Descripción
`password`	string	Contraseña de usuario del administrador de vCenter Single Sign-On, administrator@*su_nombre_de_dominio*. ■ Si implementa una instancia de vCenter Server Appliance con una instancia integrada de Platform Services Controller o un dispositivo de Platform Services Controller como la primera instancia en un dominio de vCenter Single Sign-On nuevo, debe establecer la contraseña para el usuario administrador de vCenter Single Sign-On. La contraseña debe tener entre 8 y 20 caracteres, y debe contener al menos uno de los siguientes tipos de carácter: una mayúscula, una minúscula, un número y un carácter especial, como por ejemplo, un signo de dólar ($), un numeral (#), una arroba (@), un punto (.) o un signo de exclamación (!). Todos los caracteres deben ser caracteres ASCII. ■ Si implementa un dispositivo de Platform Services Controller como partner de replicación en un dominio de vCenter Single Sign-On existente, debe proporcionar la contraseña del usuario administrador de vCenter Single Sign-On de la instancia de Platform Services Controller partner. ■ Si implementa una instancia de vCenter Server Appliance con una instancia externa de Platform Services Controller, debe proporcionar la contraseña del usuario administrador de vCenter Single Sign-On de la instancia externa de Platform Services Controller.
`domain-name`	string	Nombre de dominio de vCenter Single Sign-On, por ejemplo, vsphere.local. ■ Si implementa una instancia de vCenter Server Appliance con una instancia integrada de Platform Services Controller o un dispositivo de Platform Services Controller como la primera instancia en un dominio de vCenter Single Sign-On nuevo, debe establecer el nombre del dominio de vCenter Single Sign-On nuevo. ■ Si implementa vCenter Server Appliance con una instancia externa de Platform Services Controller o un dispositivo de Platform Services Controller como partner de replicación en un dominio de vCenter Single Sign-On existente, debe proporcionar el nombre del dominio de vCenter Single Sign-On existente.

Tabla 3-14. Parámetros de configuración en la sección `new.vcsa`, subsección `sso` (continuación)

Nombre	Tipo	Descripción
`first-instance`	Booleano	Solo es necesario si implementa un dispositivo de Platform Services Controller. El valor predeterminado es `true`. Se establece en `false` si se desea unir el dispositivo de Platform Services Controller a un dominio de vCenter Single Sign-On existente. Las instancias de Platform Services Controller unidas replican sus datos de infraestructura y habilitan Enhanced Linked Mode. Para obtener información sobre cómo administrar los servicios de Platform Services Controller, consulte *Administrar Platform Services Controller*.
`platform.services.controller`	string	El nombre de sistema de la instancia externa de Platform Services Controller. Solo es necesario si implementa una instancia externa de vCenter Server Appliancecon una instancia externa de Platform Services Controller.
`replication-partner-hostname`	string	El nombre del sistema de la instancia de Platform Services Controller partner. Solo es necesario si implementa un dispositivo de Platform Services Controller como partner de replicación en un dominio de vCenter Single Sign-On existente.
`sso.port`	entero	El puerto de proxy inverso HTTPS de la instancia de Platform Services Controller partner. El puerto predeterminado es 443. Se utiliza únicamente si la instancia de Platform Services Controller partner usa un puerto de proxy inverso HTTPS personalizado.
`site-name`	string	Nombre del sitio de vCenter Single Sign-On. Solo es necesario si se realiza una implementación de vCenter Server Appliance con una instancia integrada de Platform Services Controller o un dispositivo de Platform Services Controller. **Nota** Al configurar una instancia de Embedded Linked Mode, utilice **`Primer sitio predeterminado`** como el nombre del sitio para la primera instancia.

Parámetros de configuración en la sección `ceip`

Tabla 3-15. Parámetros de configuración en la sección `ceip`, subsección `settings`

Nombre	Tipo	Descripción
`ceip.enabled`	Booleano	Se establece en `true` para unirse al CEIP para este dispositivo.

Implementar una instancia de vCenter Server Appliance o un dispositivo de Platform Services Controller mediante la CLI

Es posible utilizar el instalador de CLI para ejecutar una implementación sin supervisión de una instancia de vCenter Server Appliance o de un dispositivo de Platform Services Controller. Se debe ejecutar la implementación de CLI desde un equipo Windows, Linux o Mac que se encuentre en la misma red en la que se desea implementar el dispositivo.

Requisitos previos

- Consulte Requisitos previos para implementar vCenter Server Appliance o el dispositivo de Platform Services Controller.
- Preparar el archivo de configuración JSON para la implementación de CLI.
- Revise Sintaxis del comando de implementación de CLI.
- Compruebe que el nombre de usuario con el que inició sesión en el equipo cliente, la ruta de acceso al instalador de vCenter Server Appliance, la ruta de acceso al archivo de configuración JSON y los valores de cadena en el archivo de configuración JSON solo contengan caracteres ASCII. No se admiten los caracteres ASCII extendidos ni los caracteres que no sean ASCII.

Procedimiento

1 Desplácese hasta el subdirectorio `vcsa-cli-installer` del sistema operativo.

   - Si la implementación se ejecuta en un sistema operativo Windows, desplácese hasta el directorio `vcsa-cli-installer\win32`.
   - Si la implementación se ejecuta en un sistema operativo Linux, desplácese hasta el directorio `vcsa-cli-installer/lin64`.
   - Si la implementación se ejecuta en el sistema operativo Mac, desplácese hasta el directorio `vcsa-cli-installer/mac`.

2 (opcional) Ejecute una comprobación previa a la implementación sin implementar el dispositivo para verificar que se haya preparado la plantilla de implementación correctamente.

```
vcsa-deploy install --verify-only path_to_the_json_file
```

3 Ejecute el comando de implementación.

```
vcsa-deploy install --accept-eula --acknowledge-ceip optional_arguments
path_to_the_json_file
```

   Utilice *optional_arguments* para introducir argumentos separados por espacios con el fin de establecer parámetros de ejecución adicionales para el comando de implementación.

   Por ejemplo, puede establecer la ubicación del registro y otros archivos de salida generados por el instalador.

```
vcsa-deploy install --accept-eula --acknowledge-ceip --log-dir=path_to_the_location
path_to_the_json_file
```

Sintaxis del comando de implementación de CLI

Puede usar argumentos de comandos para establecer los parámetros de ejecución del comando de implementación.

Puede agregar una lista de argumentos separados por un espacio en el comando de implementación de CLI.

```
vcsa-deploy install path_to_the_json_filelist_of_arguments
```

Argumento	Descripción
`--accept-eula`	Acepta el contrato de licencia de usuario final. Se requiere para ejecutar el comando de implementación.
`--acknowledge-ceip`	Confirma que el usuario acepta participar en el programa de mejora de la experiencia de cliente (CEIP) de VMware. Se requiere si el parámetro `ceip.enabled` se establece como `true` en la plantilla de implementación JSON.
`-v`, `--verbose`	Agrega información de depuración a la salida de la consola.
`-t`, `--terse`	Oculta la salida de la consola. Solo muestra mensajes de error y advertencia.
`--log-dir`*LOG_ DIR*	Establece la ubicación del registro y de otros archivos de salida.
`--skip-ovftool-verification`	Realiza una comprobación básica de los parámetros de configuración en el archivo JSON e implementa el dispositivo. No verifica los parámetros de OVF Tool.
`--no-esx-ssl-verify`	Omite la verificación de SSL para las conexiones de ESXi. **Importante** Evite utilizar esta opción, ya que puede provocar problemas durante o después de la implementación a causa de la identidad no validada del host ESXi de destino.
`--deployment-target-ssl-thumbprint`*TARGET_ THUMBPRINT*	Es la huella digital que se transfiere a OVF Tool para comprobar el host ESXi de destino o la instancia de vCenter Server donde se desea implementar el dispositivo.
`--pause-on-warnings`	Realiza una pausa y espera hasta que se acepten las advertencias.
`--verify-only`	Realiza una verificación básica de los parámetros de configuración en el archivo JSON y la verificación de los parámetros de OVF Tool. No implementa el dispositivo.
`--sso-ssl-thumbprint`*SSL-SHA1-THUMBPRINT*	Valida el certificado del servidor con respecto a la huella digital SHA1 provista.
`-h`, `--help`	Muestra el mensaje de ayuda del comando `vcsa-deploy install`.
`--template-help`	Muestra el mensaje de ayuda para el uso de parámetros de configuración del archivo de implementación JSON.

Una vez finalizada la ejecución, se puede obtener el código de salida del comando.

Código de salida	Descripción
0	Comando ejecutado correctamente
1	Error de tiempo de ejecución
2	Error de validación
3	Error en la plantilla

Instalar vCenter Server y Platform Services Controller en Windows

4

Puede instalar vCenter Server con una instancia integrada o externa de Platform Services Controller en una máquina virtual o un servidor físico de Microsoft Windows para administrar el entorno de vSphere.

Antes de instalar vCenter Server, descargue el archivo ISO del instalador y móntelo en el equipo host Windows donde desea realizar la instalación y, a continuación, inicie el asistente de instalación.

Las instalaciones en Windows de vCenter Server pueden utilizar una base de datos de PostgreSQL integrada o una base de datos externa. Antes de instalar la instancia de vCenter Server que utiliza una base de datos externa, debe preparar la base de datos. Consulte Preparar las bases de datos de vCenter Server para la instalación.

Para obtener información sobre los requisitos de vCenter Server, consulte Requisitos de vCenter Server para Windows.

Para obtener información sobre las entradas requeridas durante la instalación de vCenter Server, consulte Información necesaria para instalar vCenter Server o Platform Services Controller en Windows.

Importante Para usar topologías con instancias externas de Platform Services Controller, es necesario instalar las instancias de replicación de Platform Services Controller en secuencia. Después de implementar correctamente todas las instancias de Platform Services Controller en el dominio, se pueden realizar instalaciones simultáneas de varias instancias de vCenter Server que apuntan a una instancia externa común de Platform Services Controller.

Después de instalar vCenter Server, solo el usuario administrator@*your_domain_name* tiene privilegios para iniciar sesión en el sistema vCenter Server.

El usuario administrator@*your_domain_name* puede realizar las siguientes tareas:

- Agregar un origen de identidad en el que los usuarios y grupos adicionales se definen en vCenter Single Sign-On.
- Asignar roles a usuarios y grupos para concederles privilegios.

Para obtener información sobre cómo agregar orígenes de identidad y conceder permisos a usuarios y grupos, consulte *Administrar Platform Services Controller*.

A partir de vSphere 6.5, vCenter Server admite entornos IPv4 e IPv6 mixtos. Si desea configurar la instancia de vCenter Server para usar una versión de dirección IPv6, utilice el nombre de dominio completo (FQDN) o el nombre de host del equipo host. Para configurar una dirección IPv4, la práctica recomendada es usar el FQDN o nombre de host del equipo host, ya que la dirección IP puede cambiar si se asigna mediante DHCP.

Este capítulo incluye los siguientes temas:

Requisitos de vCenter Server para Windows

Para instalar vCenter Server en una máquina virtual o servidor físico Windows, el sistema debe cumplir con requisitos específicos de hardware y software.

- Sincronice los relojes de las máquinas virtuales en las que tiene pensado instalar vCenter Server y Platform Services Controller. Consulte Sincronizar los relojes en la red de vSphere.
- Compruebe que el nombre de DNS de la máquina virtual o del servidor físico coincida con el nombre completo del equipo.
- Compruebe que el nombre de host de la máquina virtual o del servidor físico donde va a instalar o actualizar vCenter Server cumpla con las directrices de RFC 1123..
- Compruebe que el sistema en el cual va a instalar vCenter Server no sea una controladora de dominio de Active Directory.
- Si tiene pensado utilizar una cuenta de usuario distinta de la cuenta del sistema local en el que se va a ejecutar el servicio de vCenter Server, compruebe que la cuenta de usuario tenga los siguientes permisos:
  - **Miembro del grupo de administradores**
  - **Iniciar sesión como servicio**
  - **Actuar como parte del sistema operativo (si el usuario es un usuario de dominio)**

Nota A partir de vSphere 6.5, los servicios de vCenter Server se ejecutan como procesos secundarios del servicio VMware Service Lifecycle Manager.

- Compruebe que la directiva local de la máquina virtual o del servidor físico donde va a instalar o actualizar vCenter Server permita la asignación de derechos de **Inicio de sesión como un trabajo por lotes** para nuevos usuarios locales.

  Nota A partir de vSphere 6.5, algunos procesos de vCenter Server usan distintos usuarios locales que se crean automáticamente y se agregan a la directiva de seguridad local, **Inicio de sesión como un trabajo por lotes**. Estos nuevos usuarios locales son content-library, eam, imagebuilder, mbcs, netdumper, perfcharts, rbd, vapiEndpoint, vmware-vpostgres, vsan-health, vsm, vsphere-client, and vsphere-ui.

- Si el sistema que usa para su instalación de vCenter Server pertenece a un grupo de trabajo en lugar de a un dominio, algunas funcionalidades no estarán disponible para vCenter Server. Si se asigna a un grupo de trabajo, el sistema de vCenter Server no puede detectar todos los dominios y sistemas disponibles en la red cuando se usan algunas características. En caso de que se deseen agregar orígenes de identidad de Active Directory después de la instalación, el equipo host debe estar conectado a un dominio.
- Compruebe que la cuenta LOCAL SERVICE tenga permisos de lectura en la carpeta en la cual está instalado vCenter Server y en el registro HKLM.
- Compruebe que esté funcionando la conexión entre la máquina virtual o el servidor físico y la controladora de dominio.

Comprobaciones previas a la instalación para vCenter Server y Platform Services Controller en Windows

Cuando se instalan o actualizan vCenter Server y Platform Services Controller en Windows, el instalador realiza una comprobación previa, por ejemplo, para comprobar que exista espacio suficiente en la máquina virtual o el servidor físico donde se desea instalar o actualizar vCenter Server, y comprueba que se pueda acceder correctamente a la base de datos externa, si existe alguna.

Cuando se instala Platform Services Controller como una instancia integrada o externa, vCenter Single Sign-On se instala como parte de Platform Services Controller. Durante la instalación de una instancia externa de Platform Services Controller, el instalador brinda la opción de unirse a un dominio de servidor vCenter Single Sign-On existente. Durante la instalación de vCenter Server con una instancia externa de Platform Services Controller, el instalador solicita unirse a un dominio de servidor vCenter Single Sign-On existente. Cuando se proporciona la información sobre el servicio de vCenter Single Sign-On, el instalador utiliza la cuenta de administrador para comprobar el nombre y la contraseña del host con el fin de asegurarse de que los datos del servidor vCenter Single Sign-On que se proporcionaron puedan autenticarse antes de comenzar el proceso de instalación.

El comprobador previo a la instalación comprueba los siguientes aspectos del entorno:

- Versión de Windows
- Requisitos mínimos de procesador

- Requisitos mínimos de memoria
- Requisitos mínimos de espacio en disco
- Permisos del directorio de instalación y datos seleccionado
- Disponibilidad de puertos internos y externos
- Versión de base de datos externa
- Conectividad de base de datos externa
- Privilegios de administrador en el equipo Windows
- Las credenciales que introduce

Para obtener información sobre los requisitos mínimos de almacenamiento, consulte Requisitos de almacenamiento para vCenter Server y Platform Services Controller en Windows . Para obtener información sobre los requisitos mínimos de hardware, consulte Requisitos de hardware para vCenter Server y Platform Services Controller en Windows .

Requisitos de hardware para vCenter Server y Platform Services Controller en Windows

Cuando se instala vCenter Server o Platform Services Controller en una máquina virtual o un servidor físico donde se ejecuta Microsoft Windows, el sistema debe cumplir con requisitos de hardware específicos.

Puede instalar vCenter Server y Platform Services Controller en la misma máquina virtual o un servidor físico o en máquinas virtuales o servidores físicos diferentes. Cuando instala vCenter Server con una instancia de Platform Services Controller integrada, instala vCenter Server y Platform Services Controller en la misma máquina virtual o servidor físico. Al instalar vCenter Server con una instancia de Platform Services Controller externa, primero instale Platform Services Controller que contiene todos los servicios requeridos en una máquina virtual o un servidor físico y, a continuación, instale vCenter Server y los componentes de vCenter Server en otra máquina virtual o servidor físico.

Nota No se admite la instalación de vCenter Server en una unidad de red o unidad flash USB.

Tabla 4-1. Requisitos de hardware mínimos recomendados para instalar vCenter Server y Platform Services Controller en Windows

	Platform Services Controller	vCenter Server con una instancia integrada o externa de Platform Services Controller para un entorno muy pequeño (hasta 10 hosts y 100 máquinas virtuales)	vCenter Server con una instancia integrada o externa de Platform Services Controller para un entorno pequeño (hasta 100 hosts y 1.000 máquinas virtuales)	vCenter Server con una instancia integrada o externa de Platform Services Controller para un entorno mediano (hasta 400 hosts y 4.000 máquinas virtuales)	vCenter Server con una instancia integrada o externa de Platform Services Controller para un entorno grande (hasta 1.000 hosts y 10.000 máquinas virtuales)	vCenter Server con una instancia integrada o externa de Platform Services Controller para un entorno muy grande (hasta 2.000 hosts y 35.000 máquinas virtuales)
Cantidad de CPU	2	2	4	8	16	24
Memoria	4 GB de memoria RAM	10 GB de memoria RAM	16 GB de memoria RAM	24 GB de memoria RAM	32 GB de memoria RAM	48 GB de memoria RAM

Nota Si desea agregar un host ESXi con más de 512 LUN y 2.048 rutas al inventario de vCenter Server, la instancia de vCenter Server debe ser adecuada para un entorno grande o muy grande.

Para ver los requisitos de hardware de su base de datos, consulte la documentación de la base de datos. Los requisitos de la base de datos son adicionales a los requisitos de vCenter Server en caso de que la base de datos y vCenter Server se ejecuten en la misma máquina.

Requisitos de almacenamiento para vCenter Server y Platform Services Controller en Windows

Cuando se instala vCenter Server, el sistema debe cumplir unos requisitos de almacenamiento mínimos.

Los requisitos de almacenamiento por carpeta dependen del modelo de implementación que se decide instalar. Durante la instalación, se puede seleccionar una carpeta distinta a la predeterminada `C:\Archivos de programa\VMware` para instalar vCenter Server y Platform Services Controller. También es posible seleccionar una carpeta diferente a la predeterminada `C:\ProgramData\VMware\vCenterServer\` en la cual almacenar datos.

Tabla 4-2. Requisitos mínimos de almacenamiento de vCenter Server según el modelo de implementación

Carpeta predeterminada	vCenter Server con una instancia de Platform Services Controller integrada	vCenter Server con una instancia de Platform Services Controller externa	Instancia de Platform Services Controller externa
`Archivos de programa`	6 GB	6 GB	1 GB
`ProgramData`	8 GB	8 GB	2 GB
Carpeta de sistema (para almacenar en memoria caché el instalador de MSI)	3 GB	3 GB	1 GB

Requisitos de software para vCenter Server y Platform Services Controller en Windows

Compruebe que el sistema operativo sea compatible con vCenter Server.

vCenter Server requiere un sistema operativo de 64 bits y se necesita el DSN de sistema de 64 bits para que vCenter Server pueda conectarse a la base de datos externa.

La versión más antigua de Windows Server admitida por vCenter Server es Windows Server 2008 SP2. Windows Server debe tener instaladas las actualizaciones y revisiones más recientes. Para obtener una lista completa de los sistemas operativos compatibles, consulte http://kb.vmware.com/kb/2091273.

Requisitos de base de datos para vCenter Server en Windows

vCenter Server requiere una base de datos para almacenar y organizar datos de servidor.

Cada instancia de vCenter Server debe tener su propia base de datos. En el caso de entornos con hasta 20 hosts y 200 máquinas virtuales, puede utilizar la base de datos de PostgreSQL incluida que el instalador de vCenter Server puede instalar y configurar durante la instalación de vCenter Server. Una instalación más grande requiere una base de datos externa compatible con el tamaño del entorno.

Durante la instalación de vCenter Server debe seleccionar la instalación de la base de datos integrada o dirigir el sistema de vCenter Server a cualquier base de datos existente compatible. vCenter Server es compatible con las bases de datos de Oracle y Microsoft SQL Server.

Para obtener más información sobre las versiones de servidores de bases de datos compatibles, consulte la matriz de interoperabilidad de productos VMware en http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Puertos necesarios para vCenter Server y Platform Services Controller

El sistema vCenter Server, tanto en Windows como en el dispositivo, debe poder enviar datos a cada host administrado y recibir datos de los servicios de vSphere Web Client y Platform

Services Controller. Para permitir las actividades de migración y aprovisionamiento entre los hosts administrados, los hosts de origen y de destino deben poder recibir datos de cada uno.

Se puede acceder a vCenter Server a través de los puertos TCP y UDP predeterminados. Si administra componentes de red desde afuera de un firewall, es posible que se le pida que vuelva a configurar el firewall para permitir el acceso en los puertos necesarios. Para obtener la lista de todos los puertos y protocolos compatibles en vCenter Server, consulte la herramienta VMware Ports and Protocols™ en https://ports.vmware.com/.

Durante la instalación, si un puerto se encuentra en uso o está bloqueado mediante una lista de no permitidos, el instalador de vCenter Server mostrará un mensaje de error. Debe utilizar otro número de puerto para continuar con la instalación.

VMware utiliza los puertos designados para la comunicación. Asimismo, los hosts administrados supervisan los puertos designados para los datos desde vCenter Server. Si existe un firewall integrado entre cualquiera de estos elementos, el instalador abre los puertos durante el proceso de instalación o actualización. En el caso de firewalls personalizados, debe abrir manualmente los puertos requeridos. Si posee un firewall entre dos hosts administrados y desea realizar actividades en el origen o destino, como la migración o clonación, debe configurar un medio para que los hosts administrados puedan recibir datos.

Para configurar el sistema vCenter Server a fin de que utilice un puerto diferente donde recibir los datos de vSphere Web Client, consulte la documentación de *Administrar vCenter Server y hosts*.

Requisitos de DNS para vCenter Server y Platform Services Controller en Windows

vCenter Server, al igual que los demás servidores de red, se instala o se actualiza en un equipo host con una dirección IP fija y un nombre de DNS conocido, para que los clientes puedan acceder al servicio con confianza.

Asigne una dirección IP estática y un nombre de host al servidor de Windows que va a alojar el sistema vCenter Server. Esta dirección IP debe tener un registro de sistema de nombres de dominio (DNS) válido (interno). Al instalar vCenter Server y Platform Services Controller, debe proporcionar el nombre de dominio completo (FQDN) o la dirección IP estática del equipo host en el que va a realizar la instalación o actualización. Se recomienda utilizar el FQDN.

Asegúrese de que la búsqueda inversa de DNS devuelva un FQDN cuando se consulta con la dirección IP del equipo host en el que está instalado vCenter Server. Al instalar o actualizar vCenter Server, se produce un error en la instalación o actualización del componente de servidor web compatible con vSphere Web Client si el instalador no puede buscar el nombre de dominio completo del equipo host vCenter Server a partir de su dirección IP. La búsqueda inversa se implementa mediante registros PTR.

Si planea utilizar el FQDN para la máquina virtual o el servidor físico, debe comprobar que el FQDN se pueda resolver.

Se puede utilizar el comando `nslookup` para comprobar que el servicio de búsqueda inversa de DNS devuelva un FQDN cuando se realice una consulta con la dirección IP y que el FQDN pueda resolverse.

```
nslookup -nosearch -nodefname FQDN_or_IP_address
```

Si utiliza DHCP en lugar de una dirección IP estática para vCenter Server, asegúrese de que el nombre de equipo de vCenter Server se actualice en el servicio de nombres de dominio (DNS). Si puede hacer ping al nombre de equipo, el nombre se actualiza en DNS.

Asegúrese de que la interfaz de administración del host ESXi tenga una resolución de DNS válida desde vCenter Server y todas las instancias de vSphere Web Client. Asegúrese de que vCenter Server tenga una resolución de DNS válida desde todos los hosts ESXi y todas las instancias de vSphere Web Client.

Requisitos de software de vSphere Web Client

Asegúrese de que su explorador sea compatible con vSphere Web Client.

vSphere Web Client 6.5 requiere Adobe Flash Player versión 16 a 23. Para obtener un mejor rendimiento y soluciones de seguridad, use Adobe Flash Player 23.

VMware ha probado y admite los siguientes sistemas operativos invitados y versiones de explorador para vSphere Web Client. Para obtener el mejor rendimiento, use Google Chrome.

Tabla 4-3. Sistemas operativos invitados compatibles y versiones de explorador mínimas para vSphere Web Client

Sistema operativo	Explorador
Windows de 32 bits y 64 bits	Microsoft Edge versión 79 a 86. Mozilla Firefox versión 60 a 84. Google Chrome versión 75 a 86.
Mac OS	Microsoft Edge versión 79 a 86. Mozilla Firefox versión 60 a 84. Google Chrome versión 75 a 86.

Prepararse para instalar vCenter Server y Platform Services Controller en Windows

Antes de instalar vCenter Server o Platform Services Controller, debe descargar el archivo ISO de instalación de vCenter Server y montarlo en la máquina virtual de Windows o en el servidor físico donde desea instalar vCenter Server o Platform Services Controller.

Si planea utilizar una base de datos de vCenter Server externa, antes de instalar vCenter Server, debe establecer la base de datos.

Descargar el instalador de vCenter Server para Windows

Descargue el instalador `.iso` para vCenter Server para Windows y los componentes asociados de vCenter Server y sus herramientas de soporte.

Requisitos previos

Cree una cuenta de Customer Connect en https://my.vmware.com/web/vmware/.

Procedimiento

1 Inicie sesión en VMware Customer Connect.

2 Desplácese hasta **Productos y cuentas > Todos los productos**.

3 Busque VMware vSphere y haga clic en **Ver componentes de descarga**.

4 Seleccione una versión de VMware vSphere en el menú desplegable **Seleccionar versión**.

5 Seleccione una versión de VMware vCenter Server y haga clic en **IR A DESCARGAS**.

6 Descargue la imagen ISO de vCenter Server para Windows.

7 Confirme que md5sum sea correcto mediante una herramienta de suma de comprobación MD5.

8 Monte la imagen ISO en la máquina virtual Windows o el servidor físico donde desea instalar vCenter Server para Windows.

Preparar las bases de datos de vCenter Server para la instalación

vCenter Server requiere una base de datos para almacenar y organizar datos de servidor. Para vCenter Server en Windows, puede usar la base de datos incluida de PostgreSQL que se puede instalar y configurar junto con vCenter Server, o puede configurar una base de datos externa antes de instalar vCenter Server.

vCenter Server para Windows es compatible con Oracle y Microsoft SQL Server como bases de datos externas.

Puede configurar una base de datos externa manualmente o mediante un script. Además, el usuario del nombre del origen de datos debe tener una lista específica de permisos.

Las contraseñas de las bases de datos se almacenan en texto no cifrado en el host físico o la máquina virtual de Windows en los que se instalan vCenter Server y vCenter Server Appliance. Los archivos que contienen las contraseñas están protegidos mediante la protección del sistema operativo, lo que significa que debe ser usuario raíz de Linux o administrador local de Windows para acceder a estos archivos y leerlos.

Las instancias de vCenter Server no pueden compartir el mismo esquema de base de datos. Varias bases de datos de vCenter Server pueden residir en el mismo servidor de bases de datos o pueden distribuirse entre varios servidores de bases de datos. Para las bases de datos de Oracle, que se basan en el concepto de objetos de esquema, se pueden ejecutar varias instancias de vCenter Server en un mismo servidor de bases de datos si se tiene un propietario de esquema diferente para cada instancia de vCenter Server. También se puede usar un servidor de bases de datos dedicado de Oracle para cada instancia de vCenter Server.

No se puede instalar vCenter Server y apuntar a una base de datos externa anterior de vCenter Server. Se puede actualizar la antigua base de datos de vCenter Server a la versión más reciente actualizando solo la instancia de vCenter Server que está conectada a la base de datos. Para obtener información sobre la actualización de vCenter Server, consulte *Actualizar vSphere*.

Notas sobre la configuración de la base de datos de vCenter Server

Después de seleccionar un tipo de base de datos compatible, asegúrese de comprender los requisitos de configuración especiales.

Tabla 4-4. Notas sobre la configuración de bases de datos compatibles con vCenter Server no es una lista completa de bases de datos compatibles con vCenter Server para Windows. Para obtener información sobre las versiones de bases de datos y las configuraciones de service pack específicas compatibles con vCenter Server, consulte las matrices de interoperabilidad de productos VMware. En Tabla 4-4. Notas sobre la configuración de bases de datos compatibles con vCenter Server solo se proporcionan notas de configuración de bases de datos especiales que no se enumeran en las matrices de interoperabilidad de productos.

Las bases de datos de vCenter Server requieren un conjunto de códigos UTF.

Póngase en contacto con su administrador de base de datos para obtener las credenciales de base de datos adecuadas.

Tabla 4-4. Notas sobre la configuración de bases de datos compatibles con vCenter Server

Tipo de base de datos	Notas sobre la configuración
PostgreSQL integrado	Para vCenter Server6.5, la base de datos incluida de PostgreSQL es adecuada para entornos con hasta 20 hosts y 200 máquinas virtuales. **Importante** Si utiliza la base de datos integrada de PostgreSQL, al desinstalar vCenter Server en Windows, se desinstalará la base de datos integrada y se perderán todos los datos.
Microsoft SQL Server 2008 R2 SP2 o superior	Asegúrese de que el equipo tenga una entrada de DSN de ODBC válida.
Microsoft SQL Server 2012	Asegúrese de que el equipo tenga una entrada de DSN de ODBC válida.
Microsoft SQL Server 2014	Asegúrese de que el equipo tenga una entrada de DSN de ODBC válida.
Oracle 11g y Oracle 12c	Asegúrese de que el equipo tenga una entrada de DSN de ODBC válida. Después de completar la instalación de vCenter Server, aplique la última revisión al cliente y el servidor de Oracle.

Configurar bases de datos de Microsoft SQL Server

Si desea usar una base de datos de Microsoft SQL para su repositorio de vCenter Server, configure la base de datos que funcionará con vCenter Server.

Puede instalar y configurar la base de datos Microsoft SQL Server en el mismo equipo en el que instalará vCenter Server. Puede instalar y configurar la base de datos Microsoft SQL Server en otro equipo.

Procedimiento

1 Preparar la base de datos de SQL Server de vCenter Server

   Primero debe crear una base de datos y un usuario para vCenter Server. A continuación, podrá asignar permisos al usuario de base de datos de vCenter Server mediante el esquema de dbo y la función dbo_owner existentes, o mediante la creación de un esquema y unas funciones de base de datos personalizados.

2 (opcional) Usar un script para crear manualmente objetos de base de datos de Microsoft SQL Server

   En este tema se describe la creación de objetos de base de datos de forma manual, en vez de permitir la creación automática de los mismos por parte del instalador de vCenter Server.

3 Configurar una conexión de ODBC de SQL Server

   Tras crear y configurar una base de datos de SQL Server y un usuario para vCenter Server, debe crear un DSN de 64 bits en el equipo en el que instalará vCenter Server. Durante la instalación de vCenter Server, usará el DSN para establecer una conexión entre vCenter Server y la base de datos.

4 Configurar TCP/IP de Microsoft SQL Server para JDBC

   Si la base de datos de Microsoft SQL Server posee TCP/IP deshabilitado y no se configuran los puertos dinámicos, la conexión JDBC permanece cerrada. La conexión cerrada provoca un funcionamiento incorrecto de las estadísticas de vCenter Server. Puede configurar TCP/IP del servidor para JDBC.

Preparar la base de datos de SQL Server de vCenter Server

Primero debe crear una base de datos y un usuario para vCenter Server. A continuación, podrá asignar permisos al usuario de base de datos de vCenter Server mediante el esquema de dbo y la función dbo_owner existentes, o mediante la creación de un esquema y unas funciones de base de datos personalizados.

Requisitos previos

Inicie sesión en Microsoft SQL Server Management Studio como sysadmin (SA) o con una cuenta de usuario con privilegios sysadmin.

Preparar la base de datos de vCenter Server mediante el esquema dbo y la función de base de datos db_owner

El modo más sencillo de asignar permisos a un usuario de la base de datos de vCenter Server es mediante la función de base de datos db_owner.

Primero debe crear una base de datos y un usuario para vCenter Server. A continuación, podrá usar la función de base de datos dbo_owner y permitir que el instalador de vCenter Server cree el esquema de dbo predeterminado que asigna los permisos de usuario de base de datos a dicha función. También debe habilitar la supervisión de la base de datos del usuario antes de instalar vCenter Server. Consulte Requisitos de permisos de base de datos para vCenter Server.

Para realizar el siguiente procedimiento, puede usar la interfaz de usuario gráfica o ejecutar scripts. El paquete del instalador de vCenter Server contiene scripts de ejemplo en el archivo `vCenter-Server\dbschema\DB_and_schema_creation_scripts_PostgreSQL.txt`.

Procedimiento

1 Cree una base de datos y un usuario para vCenter Server.

   a En la base de datos principal, cree una base de datos para vCenter Server.

   b Cree un usuario de base de datos para vCenter Server y asígnelo a las bases de datos de vCenter Server y msdb.

   Por ejemplo, para crear el VCDB de la base de datos y el usuario vpxuser, puede ejecutar el siguiente script:

```
use master
go
CREATE DATABASE VCDB ON PRIMARY
(NAME = N'vcdb', FILENAME = N'C:\database_path\VCDB.mdf', SIZE = 10MB, FILEGROWTH = 10% )
LOG ON
(NAME = N'vcdb_log', FILENAME = N'C:\database_path\VCDB.ldf', SIZE = 1000KB, FILEGROWTH =
10%)
COLLATE SQL_Latin1_General_CP1_CI_AS
go
use VCDB
go
CREATE LOGIN vpxuser WITH PASSWORD=N'vpxuser!0', DEFAULT_DATABASE=VCDB,
DEFAULT_LANGUAGE=us_english, CHECK_POLICY=OFF
go
CREATE USER vpxuser for LOGIN vpxuser
go
use MSDB
go
CREATE USER vpxuser for LOGIN vpxuser
go
```

   Ahora tiene una base de datos Microsoft SQL Server que puede utilizar con vCenter Server.

2 Asigne la función db_owner al usuario de la base de datos de vCenter Server en las bases de datos de vCenter Server y msdb.

   Por ejemplo, para asignar la función db_owner al usuario vpxuser, puede ejecutar el siguiente script:

```
use VCDB
go
sp_addrolemember @rolename = 'db_owner', @membername = 'vpxuser'
go
use MSDB
go
sp_addrolemember @rolename = 'db_owner', @membername = 'vpxuser'
go
```

3 Habilite la supervisión de la base de datos para el usuario de base de datos de vCenter Server.

   Por ejemplo, para conceder permisos de supervisión de tamaño del disco de la base de datos, puede ejecutar el siguiente script:

```
use master
go
grant VIEW SERVER STATE to vpxuser
go
GRANT VIEW ANY DEFINITION TO vpxuser
go
```

Resultados

Cuando se instala vCenter Server, el instalador usa el esquema dbo predeterminado para asignar permisos a la función db_owner.

Preparar la base de datos de vCenter Server mediante la creación de un esquema y unas funciones de base de datos personalizados

Como alternativa al uso de la función de base de datos db_owner, los administradores de bases de datos con experiencia pueden establecer permisos mediante la creación del esquema y las funciones de base de datos de forma manual, lo que permite un mayor control sobre los permisos de la base de datos.

Primero debe crear una base de datos y un usuario para vCenter Server. A continuación, podrá crear un esquema personalizado y nuevas funciones de base de datos para el usuario de la base de datos. También debe habilitar la supervisión de la base de datos del usuario antes de instalar vCenter Server. Consulte Requisitos de permisos de base de datos para vCenter Server.

Para realizar el siguiente procedimiento, puede usar la interfaz de usuario gráfica o ejecutar scripts. El paquete del instalador de vCenter Server contiene scripts de ejemplo en el archivo `vCenter-Server\dbschema\DB_and_schema_creation_scripts_PostgreSQL.txt`.

Procedimiento

1 Cree una base de datos y un usuario para vCenter Server.

   a En la base de datos principal, cree una base de datos para vCenter Server.

   b Cree un usuario de base de datos para vCenter Server y asígnelo a las bases de datos de vCenter Server y msdb.

   Por ejemplo, para crear el VCDB de la base de datos y el usuario vpxuser, puede ejecutar el siguiente script:

```
use master
go
CREATE DATABASE VCDB ON PRIMARY
(NAME = N'vcdb', FILENAME = N'C:\database_path\VCDB.mdf', SIZE = 10MB, FILEGROWTH = 10% )
LOG ON
(NAME = N'vcdb_log', FILENAME = N'C:\database_path\VCDB.ldf', SIZE = 1000KB, FILEGROWTH =
10%)
COLLATE SQL_Latin1_General_CP1_CI_AS
go
use VCDB
go
CREATE LOGIN vpxuser WITH PASSWORD=N'vpxuser!0', DEFAULT_DATABASE=VCDB,
DEFAULT_LANGUAGE=us_english, CHECK_POLICY=OFF
go
CREATE USER vpxuser for LOGIN vpxuser
go
use MSDB
go
CREATE USER vpxuser for LOGIN vpxuser
go
```

   Ahora tiene una base de datos Microsoft SQL Server que puede utilizar con vCenter Server.

2 En la base de datos de vCenter Server, cree un esquema de base de datos y asígnelo al usuario de base de datos de vCenter Server.

   Por ejemplo, para crear el esquema VMW en VCDB y asignarlo al usuario vpxuser, puede ejecutar el siguiente script:

```
use VCDB
CREATE SCHEMA VMW
go
ALTER USER vpxuser WITH DEFAULT_SCHEMA =VMW
```

3 En la base de datos de vCenter Server, cree privilegios y asígnelos a las funciones de base de datos VC_ADMIN_ROLE y VC_USER_ROLE; a continuación, asigne dichas funciones al usuario de base de datos de vCenter Server.

Por ejemplo, para crear las funciones de VCDB y asignarlas al usuario vpxuser, puede ejecutar el siguiente script:

```
use VCDB
go
if not exists (SELECT name FROM sysusers WHERE issqlrole=1 AND name = 'VC_ADMIN_ROLE')
CREATE ROLE VC_ADMIN_ROLE;
GRANT ALTER ON SCHEMA :: VMW to VC_ADMIN_ROLE;
GRANT REFERENCES ON SCHEMA :: VMW to VC_ADMIN_ROLE;
GRANT INSERT ON SCHEMA ::  VMW to VC_ADMIN_ROLE;

GRANT CREATE TABLE to VC_ADMIN_ROLE;
GRANT CREATE VIEW to VC_ADMIN_ROLE;
GRANT CREATE Procedure to VC_ADMIN_ROLE;

if not exists (SELECT name FROM sysusers WHERE issqlrole=1 AND name = 'VC_USER_ROLE')
CREATE ROLE VC_USER_ROLE
go
GRANT SELECT ON SCHEMA ::  VMW to VC_USER_ROLE
go
GRANT INSERT ON SCHEMA ::  VMW to VC_USER_ROLE
go
GRANT DELETE ON SCHEMA ::  VMW to VC_USER_ROLE
go
GRANT UPDATE ON SCHEMA ::  VMW to VC_USER_ROLE
go
GRANT EXECUTE ON SCHEMA :: VMW to VC_USER_ROLE
go
sp_addrolemember VC_USER_ROLE , vpxuser
go
sp_addrolemember VC_ADMIN_ROLE , vpxuser
go
```

4 En la base de datos de msdb, cree privilegios y asígnelos a la función de base de datos VC_ADMIN_ROLE; a continuación, asigne dicha función al usuario de base de datos de vCenter Server.

Por ejemplo, para crear las funciones y asignarlas al usuario vpxuser, puede ejecutar el siguiente script:

```
use MSDB
go
if not exists (SELECT name FROM sysusers WHERE issqlrole=1 AND name = 'VC_ADMIN_ROLE')
CREATE ROLE VC_ADMIN_ROLE;
go
GRANT SELECT on msdb.dbo.syscategories to VC_ADMIN_ROLE
go
GRANT SELECT on msdb.dbo.sysjobsteps to VC_ADMIN_ROLE
go
GRANT SELECT ON msdb.dbo.sysjobs to VC_ADMIN_ROLE
```

```
go
GRANT SELECT ON msdb.dbo.sysjobs_view to VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_job TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_delete_job TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_jobstep TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_update_job TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_jobserver TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_jobschedule TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_category TO VC_ADMIN_ROLE
go
sp_addrolemember VC_ADMIN_ROLE , vpxuser
go
```

Nota La función VC_ADMIN_ROLE de la base de datos de msdb solo es necesaria durante la instalación y la actualización de vCenter Server. Tras la instalación o la actualización, puede retirar la función y desactivarla para futuras actualizaciones, o puede quitarla para mejorar la seguridad.

5 Habilite la supervisión de la base de datos para el usuario de base de datos de vCenter Server.

Por ejemplo, para conceder permisos de supervisión de tamaño del disco de la base de datos, puede ejecutar el siguiente script:

```
use master
go
grant VIEW SERVER STATE to vpxuser
go
GRANT VIEW ANY DEFINITION TO vpxuser
go
```

Usar un script para crear manualmente objetos de base de datos de Microsoft SQL Server

En este tema se describe la creación de objetos de base de datos de forma manual, en vez de permitir la creación automática de los mismos por parte del instalador de vCenter Server.

Procedimiento

1 Inicie sesión en Microsoft SQL Server Management Studio con la cuenta de usuario de base de datos de vCenter Server que creó en las bases de datos de vCenter Server y msdb.

2 En el paquete de instalación de vCenter Server, busque los scripts de dbschema en el directorio `vCenter-Server/dbschema`.

3 Abra los archivos `VCDB_mssql.SQL` y `TopN_DB_mssql.sql` con Microsoft SQL Server Management Studio y reemplace todas las ocurrencias de `$schema` con el nombre del esquema.

4 Abra el archivo `VCDB_views_mssql.sql` con Microsoft SQL Server Management Studio y, tras cada una de las ocurrencias de `;`, inserte una nueva línea y escriba `go`.

5 Ejecute los scripts en una secuencia en la base de datos.

   El usuario de DBO debe ser el propietario de los objetos que se crearon con estos scripts. Abra los scripts uno a uno en Microsoft SQL Server Management Studio y pulse F5 para ejecutar cada script en el siguiente orden:

   a `VCDB_mssql.SQL`
   b `insert_stats_proc_mssql.sql`
   c `load_stats_proc_mssql.sql`
   d `purge_stat2_proc_mssql.sql`
   e `purge_stat3_proc_mssql.sql`
   f `purge_usage_stats_proc_mssql.sql`
   g `stats_rollup1_proc_mssql.sql`
   h `stats_rollup2_proc_mssql.sql`
   i `stats_rollup3_proc_mssql.sql`
   j `cleanup_events_mssql.sql`
   k `delete_stats_proc_mssql.sql`
   l `upsert_last_event_proc_mssql.sql`
   m `load_usage_stats_proc_mssql.sql`
   n `TopN_DB_mssql.sql`
   o `calc_topn1_proc_mssql.sql`
   p `calc_topn2_proc_mssql.sql`
   q `calc_topn3_proc_mssql.sql`
   r `calc_topn4_proc_mssql.sql`
   s `clear_topn1_proc_mssql.sql`
   t `clear_topn2_proc_mssql.sql`
   u `clear_topn3_proc_mssql.sql`
   v `clear_topn4_proc_mssql.sql`
   w `rule_topn1_proc_mssql.sql`
   x `rule_topn2_proc_mssql.sql`
   y `rule_topn3_proc_mssql.sql`

z `rule_topn4_proc_mssql.sql`

aa `process_license_snapshot_mssql.sql`

ab `l_stats_rollup3_proc_mssql.sql`

ac `l_purge_stat2_proc_mssql.sql`

ad `l_purge_stat3_proc_mssql.sql`

ae `l_stats_rollup1_proc_mssql.sql`

af `l_stats_rollup2_proc_mssql.sql`

ag `VCDB_views_mssql.sql`

6 (opcional) Ejecute los scripts para habilitar la supervisión del estado de la base de datos.

a `job_dbm_performance_data_mssql.sql`

b `process_performance_data_mssql.sql`

7 Para todas las ediciones compatibles de Microsoft SQL Server, excepto Microsoft SQL Server Express, ejecute los scripts para configurar trabajos programados en la base de datos.

Estos scripts aseguran que el servicio de SQL Server Agent esté en ejecución.

a `job_schedule1_mssql.sql`

b `job_schedule2_mssql.sql`

c `job_schedule3_mssql.sql`

d `job_cleanup_events_mssql.sql`

e `job_topn_past_day_mssql.sql`

f `job_topn_past_week_mssql.sql`

g `job_topn_past_month_mssql.sql`

h `job_topn_past_year_mssql.sql`

8 Para todos los procedimientos que creó en Paso 5, otorgue el privilegio de ejecución al usuario de base de datos de vCenter Server en la base de datos vCenter Server.

Por ejemplo, para conceder el permiso de ejecución de los procedimientos al usuario y vpxuser, puede ejecutar el siguiente script.

```
grant execute on insert_stats_proc to vpxuser
grant execute on purge_stat2_proc to vpxuser
grant execute on purge_stat3_proc to vpxuser
grant execute on purge_usage_stat_proc to vpxuser
grant execute on stats_rollup1_proc to vpxuser
grant execute on stats_rollup2_proc to vpxuser
grant execute on stats_rollup3_proc to vpxuser
grant execute on cleanup_events_tasks_proc to vpxuser
grant execute on delete_stats_proc to vpxuser
grant execute on upsert_last_event_proc to vpxuser
```

```
grant execute on load_usage_stats_proc to vpxuser
grant execute on load_stats_proc to vpxuser
grant execute on calc_topn1_proc to vpxuser
grant execute on calc_topn2_proc to vpxuser
grant execute on calc_topn3_proc to vpxuser
grant execute on calc_topn4_proc to vpxuser
grant execute on clear_topn1_proc to vpxuser
grant execute on clear_topn2_proc to vpxuser
grant execute on clear_topn3_proc to vpxuser
grant execute on clear_topn4_proc to vpxuser
grant execute on rule_topn1_proc to vpxuser
grant execute on rule_topn2_proc to vpxuser
grant execute on rule_topn3_proc to vpxuser
grant execute on rule_topn4_proc to vpxuser
grant execute on process_license_snapshot_proc to vpxuser
grant execute on l_stats_rollup3_proc to vpxuser
grant execute on l_purge_stat2_proc to vpxuser
grant execute on l_purge_stat3_proc to vpxuser
grant execute on l_stats_rollup1_proc to vpxuser
grant execute on l_stats_rollup2_proc to vpxuser
```

Si se ejecutó el script `process_performance_data_mssql.sql` en Paso 5, otorgue el siguiente privilegio de ejecución a la base de datos de vCenter Server.

```
grant execute on process_performance_data_proc to vpxuser
```

Resultados

Ha creado las tablas de vCenter Server de forma manual.

Nota Durante la instalación de vCenter Server, cuando aparezca el mensaje de advertencia de reinicialización, seleccione **No sobrescribir, dejar la base de datos existente como está** y continúe con la instalación.

Configurar una conexión de ODBC de SQL Server

Tras crear y configurar una base de datos de SQL Server y un usuario para vCenter Server, debe crear un DSN de 64 bits en el equipo en el que instalará vCenter Server. Durante la instalación de vCenter Server, usará el DSN para establecer una conexión entre vCenter Server y la base de datos.

Si usa SQL Server para vCenter Server, no utilice la base de datos maestra ni ninguna otra base de datos del sistema.

Consulte la documentación de ODBC de Microsoft SQL para obtener instrucciones específicas para configurar la conexión de ODBC de SQL Server.

Precaución Si está usando una instancia con nombre de Microsoft SQL Server 2008 Standard Edition con vCenter Server, no coloque el nombre MSSQLSERVER a la instancia. Si lo hace, la conexión JDBC no funciona y ciertas funciones, como Gráficos de rendimiento, no están disponibles.

Requisitos previos

Implementar SQL Native Client versión 10 u 11.

Procedimiento

1. En el equipo en el que instalará vCenter Server, seleccione **Inicio > Herramientas de administración > Orígenes de datos (ODBC)**.
2. En la pestaña **DSN del sistema**, modifique una conexión de ODBC de SQL Server existente o cree una nueva.
   - Para modificar una conexión de ODBC de SQL Server existente, seleccione la conexión desde la lista Origen de datos del sistema y haga clic en **Configurar**.

     Importante El DSN existente debe usar SQL Native Client versión 10 u 11.
   - Para crear una nueva conexión de ODBC de SQL Server, haga clic en **Agregar**, seleccione **SQL Native Client** y presione en **Finalizar**.
3. En el cuadro de texto **Nombre**, introduzca un nombre para el origen de datos ODBC (DSN).

   Por ejemplo, **`VMware vCenter Server`**.
4. (opcional) En el cuadro de texto **Descripción**, introduzca una descripción del DSN de ODBC.
5. En el cuadro de texto **Servidor**, introduzca la dirección IP o FQDN de SQL Server y, si desea utilizar un puerto no predeterminado para acceder a SQL Server, introduzca un puerto personalizado separado con una coma.

   Por ejemplo, si la dirección IP de SQL Server es 10.160.10.160 y desea acceder al servidor mediante el puerto personalizado 8347, introduzca **`10.160.10.160,8347`**.

   Nota No se puede usar un alias de servidor de base de datos para crear un DSN.
6. Seleccione un método de autenticación.
   - **Integrar autenticación de Windows**.

     Además, también puede escribir el nombre principal de servicio (SPN, Service Principal Name).

     Importante No puede utilizar esta opción si el servicio vCenter Server se ejecuta en una cuenta del sistema integrada de Microsoft Windows.
   - **Autenticación de SQL Server**.

     Introduzca su nombre de inicio de sesión y contraseña de SQL Server.
7. Seleccione la base de datos creada para el sistema vCenter Server en el menú **Cambiar la base de datos predeterminada a**.
8. Haga clic en **Finalizar**.

9 Pruebe el origen de los datos. Para ello, seleccione **Probar origen de datos** y haga clic en **Aceptar** en el menú **Configuración de Microsoft SQL Server de ODBC**.

10 Compruebe que SQL Agent esté en ejecución en el servidor de base de datos.

Configurar TCP/IP de Microsoft SQL Server para JDBC

Si la base de datos de Microsoft SQL Server posee TCP/IP deshabilitado y no se configuran los puertos dinámicos, la conexión JDBC permanece cerrada. La conexión cerrada provoca un funcionamiento incorrecto de las estadísticas de vCenter Server. Puede configurar TCP/IP del servidor para JDBC.

Esta tarea se aplica a los servidores de base de datos remotos de Microsoft SQL Server. Puede omitir esta tarea si la base de datos se encuentra en el mismo equipo que vCenter Server.

Procedimiento

1 Seleccione **Inicio** > **Todos los programas** > **Microsoft SQL Server** > **Herramienta de configuración** > **Administrador de configuración de SQL Server**.

2 Seleccione **Configuración de red de SQL Server** > **Protocolos para** ***nombre de la instancia***.

3 Habilite TCP/IP.

4 Abra Propiedades de TCP/IP.

5 En la pestaña **Protocolo**, cree las siguientes entradas.

Habilitado	**Sí**
Escuchar todo	**Sí**
Mantener conexión	**30000**

6 En la pestaña **Direcciones IP**, realice las siguientes selecciones.

activa	**Sí**
Puertos dinámicos de TCP	**0**

7 Reinicie el servicio SQL Server desde **Administrador de configuración de SQL Server** > **Servicios de SQL Server**.

8 Inicie el servicio SQL Server Browser desde **Administrador de configuración de SQL** > **Server Servicios de SQL Server**.

Configurar bases de datos de Oracle

Si desea utilizar una base de datos de Oracle para el repositorio de vCenter Server, configure la base de datos para que funcione con vCenter Server.

Puede instalar y configurar la base de datos de Oracle en el mismo equipo en el que instalará vCenter Server. Puede instalar y configurar la base de datos de Oracle en otro equipo.

Procedimiento

1 Preparar la base de datos de Oracle de vCenter Server

   Para usar una base de datos de Oracle con vCenter Server, debe crear la base de datos con determinados espacios de tablas y privilegios, y el usuario de la base de datos con unos permisos concretos.

2 (opcional) Usar un script para crear un esquema de base de datos de Oracle

   El instalador de vCenter Server crea el esquema durante la instalación. Para administradores de bases de datos experimentados que necesitan más control sobre la creación de esquemas debido a limitaciones de los entornos, puede opcionalmente utilizar un script para crear su esquema de base de datos.

3 Crear un nombre del servicio de red

   Para configurar un DSN de ODBC de Oracle, debe tener un nombre del servicio de red para la base de datos. En el equipo en el que se ejecute la base de datos de Oracle, debe crear un nombre del servicio de red para el espacio de tablas de vCenter Server.

4 Configurar una conexión de ODBC de Oracle

   Tras crear y configurar una base de datos de Oracle y un usuario para vCenter Server, debe crear un DSN de 64 bits en el equipo en el que instalará vCenter Server. Durante la instalación de vCenter Server, usará el DSN para establecer una conexión entre vCenter Server y la base de datos.

Preparar la base de datos de Oracle de vCenter Server

Para usar una base de datos de Oracle con vCenter Server, debe crear la base de datos con determinados espacios de tablas y privilegios, y el usuario de la base de datos con unos permisos concretos.

Primero debe crear un espacio de tablas y un usuario para vCenter Server. A continuación, conceda los permisos al usuario de la base de datos. También debe habilitar la supervisión de la base de datos del usuario antes de instalar vCenter Server. Consulte Requisitos de permisos de base de datos para vCenter Server.

Para realizar el siguiente procedimiento, puede usar la interfaz de usuario gráfica o ejecutar scripts. El paquete del instalador de vCenter Server contiene scripts de ejemplo en el archivo `vCenter-Server\dbschema\DB_and_schema_creation_scripts_PostgreSQL.txt`.

Requisitos previos

Inicie sesión en una sesión de SQL*Plus con la cuenta del sistema.

Procedimiento

1 Cree un espacio de tablas para vCenter Server.

Por ejemplo, para crear el espacio de tablas VPX, puede ejecutar el siguiente script:

```
CREATE SMALLFILE TABLESPACE "VPX" DATAFILE 'C:\database_path\vpx01.dbf'
SIZE 1G AUTOEXTEND ON NEXT 10M MAXSIZE UNLIMITED LOGGING EXTENT MANAGEMENT LOCAL SEGMENT
SPACE MANAGEMENT AUTO;
```

2 Cree un usuario de la base de datos con los permisos adecuados para vCenter Server.

Por ejemplo, para crear el usuario VPXADMIN, puede ejecutar el siguiente script:

```
CREATE USER "VPXADMIN" PROFILE "DEFAULT" IDENTIFIED BY "oracle" DEFAULT TABLESPACE "VPX"
ACCOUNT UNLOCK;
grant connect to VPXADMIN;
grant resource to VPXADMIN;
grant create view to VPXADMIN;
grant create sequence to VPXADMIN;
grant create table to VPXADMIN;
grant create materialized view to VPXADMIN;
grant execute on dbms_lock to VPXADMIN;
grant execute on dbms_job to VPXADMIN;
grant select on dba_lock to VPXADMIN;
grant select on dba_tablespaces to VPXADMIN;
grant select on dba_temp_files to VPXADMIN;
grant select on dba_data_files to VPXADMIN;
grant select on v_$session to VPXADMIN;
grant unlimited tablespace to VPXADMIN;
```

De forma predeterminada, el rol RECURSO tiene asignados los privilegios **CREAR PROCEDIMIENTO**, **CREAR TABLA** y **CREAR SECUENCIA**. Si el rol RECURSO no posee estos privilegios, concédaselos al usuario de la base de datos de vCenter Server.

Nota En lugar de conceder espacio de tablas ilimitado, puede establecer una cuota específica de espacio de tablas. La cuota recomendada es ilimitada, con un mínimo de 500 MB. Para establecer una cuota ilimitada, utilice el siguiente comando:

```
alter user "VPXADMIN" quota unlimited on "VPX";
```

Si establece una cuota limitada, supervise el espacio de tablas restante disponible para evitar el error que se muestra a continuación.

```
ORA-01536: se superó la cuota de espacio para el espacio de tablas 'espacio de tablas'
```

De este modo, tendrá el usuario de la base de datos de Oracle para vCenter Server.

3 Habilite la supervisión de la base de datos para el usuario de base de datos de vCenter Server.

   Por ejemplo, para conceder permisos de supervisión de tamaño del disco de la base de datos al usuario VPXADMIN, puede ejecutar el siguiente script:

```
grant select on v_$system_event to VPXADMIN;
grant select on v_$sysmetric_history to VPXADMIN;
grant select on v_$sysstat to VPXADMIN;
grant select on dba_data_files to VPXADMIN;
grant select on v_$loghist to VPXADMIN;
```

Usar un script para crear un esquema de base de datos de Oracle

El instalador de vCenter Server crea el esquema durante la instalación. Para administradores de bases de datos experimentados que necesitan más control sobre la creación de esquemas debido a limitaciones de los entornos, puede opcionalmente utilizar un script para crear su esquema de base de datos.

Procedimiento

1 Abra una ventana de SQL*Plus con un usuario que posea derechos de propiedad de esquemas en la base de datos de vCenter Server.

2 Busque los scripts dbschema en el directorio `/`*`directorio de instalación`*`/vCenter-Server/dbschema` del paquete de instalación de vCenter Server.

3 En SQL*Plus, ejecute los scripts en orden en la base de datos.

   a `VCDB_oracle.SQL`

   b `VCDB_views_oracle.SQL`

   c `insert_stats_proc_oracle.sql`

   d `load_stats_proc_oracle.sql`

   e `purge_stat2_proc_oracle.sql`

   f `purge_stat3_proc_oracle.sql`

   g `purge_usage_stats_proc_oracle.sql`

   h `stats_rollup1_proc_oracle.sql`

   i `stats_rollup2_proc_oracle.sql`

   j `stats_rollup3_proc_oracle.sql`

   k `cleanup_events_oracle.sql`

   l `delete_stats_proc_oracle.sql`

   m `load_usage_stats_proc_oracle.sql`

   n `TopN_DB_oracle.sql`

o `calc_topn1_proc_oracle.sql`

p `calc_topn2_proc_oracle.sql`

q `calc_topn3_proc_oracle.sql`

r `calc_topn4_proc_oracle.sql`

s `clear_topn1_proc_oracle.sql`

t `clear_topn2_proc_oracle.sql`

u `clear_topn3_proc_oracle.sql`

v `clear_topn4_proc_oracle.sql`

w `rule_topn1_proc_oracle.sql`

x `rule_topn2_proc_oracle.sql`

y `rule_topn3_proc_oracle.sql`

z `rule_topn4_proc_oracle.sql`

aa `process_license_snapshot_oracle.sql`

ab `l_purge_stat2_proc_oracle.sql`

ac `l_purge_stat3_proc_oracle.sql`

ad `l_stats_rollup1_proc_oracle.sql`

ae `l_stats_rollup2_proc_oracle.sql`

af `l_stats_rollup3_proc_oracle.sql`

4 (opcional) También puede ejecutar los siguientes scripts para habilitar la supervisión de mantenimiento de la base de datos.

   a `job_dbm_performance_data_oracle.sql`

   b `process_performance_data_oracle.sql`

5 Para todas las ediciones compatibles de Oracle Server, ejecute los scripts para configurar los trabajos programados en la base de datos.

   a `job_schedule1_oracle.sql`

   b `job_schedule2_oracle.sql`

   c `job_schedule3_oracle.sql`

   d `job_cleanup_events_oracle.sql`

   e `job_topn_past_day_oracle.sql`

   f `job_topn_past_week_oracle.sql`

   g `job_topn_past_month_oracle.sql`

h `job_topn_past_year_oracle.sql`

Resultados

Ha creado las tablas de vCenter Server de forma manual.

Nota Durante la instalación de vCenter Server, cuando aparezca el mensaje de advertencia de reinicialización, seleccione **No sobrescribir, dejar la base de datos existente como está** y continúe con la instalación.

Crear un nombre del servicio de red

Para configurar un DSN de ODBC de Oracle, debe tener un nombre del servicio de red para la base de datos. En el equipo en el que se ejecute la base de datos de Oracle, debe crear un nombre del servicio de red para el espacio de tablas de vCenter Server.

Procedimiento

1 Use un editor de texto o el asistente de configuración de Net8 para abrir el archivo `tnsnames.ora` que se encuentra en el directorio `C:\Oracle\Oraxx\NETWORK\ADMIN`, donde *xx* corresponde a **10g** o **11g**.

2 Agregue la siguiente entrada, donde `HOST` corresponde al host administrado al que debe conectarse el cliente.

```
VPX_TNS =
(DESCRIPTION =
(ADDRESS_LIST =
(ADDRESS=(PROTOCOL=TCP)(HOST=vpxd-Oracle)(PORT=1521))
   )
(CONNECT_DATA =
(SERVICE_NAME = ORCL)
   )
   )
```

Configurar una conexión de ODBC de Oracle

Tras crear y configurar una base de datos de Oracle y un usuario para vCenter Server, debe crear un DSN de 64 bits en el equipo en el que instalará vCenter Server. Durante la instalación de vCenter Server, usará el DSN para establecer una conexión entre vCenter Server y la base de datos.

Requisitos previos

Instale Oracle Client 11.2.0.3 p16656151 (revisión 19) o una versión posterior, 11.2.0.4, 12.1.0.1.12 o posterior, o 12.1.0.2.

Procedimiento

1 En el equipo en el que instalará vCenter Server, seleccione **Inicio > Herramientas de administración > Orígenes de datos (ODBC)**.

2 En la pestaña **DSN del sistema**, modifique una conexión de ODBC de Oracle existente o cree una nueva.

- Para modificar una conexión de ODBC de Oracle existente, seleccione la conexión desde la lista Origen de datos del sistema y haga clic en **Configurar**.
- Para crear una conexión de ODBC de Oracle, haga clic en **Agregar**, seleccione el cliente Oracle y haga clic en **Finalizar**.

3 En el cuadro de texto **Nombre del origen de datos**, introduzca un nombre para el origen de datos (DSN) ODBC.

Por ejemplo, **`VMware vCenter Server`**.

4 (opcional) En el cuadro de texto **Descripción**, introduzca una descripción del DSN de ODBC.

5 En el cuadro de texto **Nombre de servicio de TNS**, escriba el nombre del servicio de red para la base de datos a la que desea conectarse.

Por ejemplo, **`VPX_TNS`**.

Este es el nombre de servicio de red que configuró anteriormente en el archivo `tnsnames.ora` que se encuentra en la carpeta `NETWORK\ADMIN` de la ubicación de instalación de la base de datos de Oracle.

6 En el cuadro de texto **Identificador de usuario**, escriba el nombre de usuario de la base de datos de vCenter Server.

Por ejemplo, **`VPXADMIN`**.

7 Haga clic en **Probar conexión**.

8 En el cuadro de texto **Contraseña**, escriba la contraseña del usuario de la base de datos y haga clic en **Aceptar**.

Si ha configurado el DNS correctamente, aparecerá el mensaje `Conexión correcta`.

9 Haga clic en **Aceptar**.

Requisitos de permisos de base de datos para vCenter Server

vCenter Server requiere una base de datos. Si decide utilizar una base de datos de Oracle o Microsoft SQL Server externa, cuando cree la base de datos, deberá conceder determinados permisos al usuario de la base de datos.

Tabla 4-5. Permisos de base de datos Microsoft SQL para vCenter Server

Permiso	Descripción
GRANT ALTER ON SCHEMA :: [VMW] TO VC_ADMIN_ROLE	Obligatorio cuando trabaja con el esquema personalizado de SQL Server.
GRANT REFERENCES ON SCHEMA :: [VMW] TO VC_ADMIN_ROLE	Obligatorio cuando trabaja con el esquema personalizado de SQL Server.
GRANT INSERT ON SCHEMA :: [VMW] TO VC_ADMIN_ROLE	Obligatorio cuando trabaja con el esquema personalizado de SQL Server.

Tabla 4-5. Permisos de base de datos Microsoft SQL para vCenter Server (continuación)

Permiso	Descripción
GRANT CREATE TABLE TO VC_ADMIN_ROLE	Necesario para crear una tabla.
GRANT CREATE VIEW TO VC_ADMIN_ROLE	Necesario para crear una vista.
GRANT CREATE PROCEDURE TO VC_ADMIN_ROLE	Necesario para crear un procedimiento almacenado.
GRANT SELECT ON SCHEMA :: [VMW] TO VC_USER_ROLE	Permisos que permiten ejecutar las operaciones SELECT, INSERT, DELETE y UPDATE en tablas que son parte del esquema VMW.
GRANT INSERT ON SCHEMA :: [VMW] TO VC_USER_ROLE	
GRANT DELETE ON SCHEMA :: [VMW] TO VC_USER_ROLE	
GRANT UPDATE ON SCHEMA :: [VMW] TO VC_USER_ROLE	
GRANT EXECUTE ON SCHEMA :: [VMW] TO VC_USER_ROLE	Necesario para ejecutar un procedimiento almacenado en el esquema de base de datos.
GRANT SELECT ON msdb.dbo.syscategories TO VC_ADMIN_ROLE	Necesario para implementar trabajos de SQL Server. Estos permisos son obligatorios solo durante la instalación y actualización y no son necesarios después de la implementación.
GRANT SELECT ON msdb.dbo.sysjobsteps TOVC_ADMIN_ROLE	
GRANT SELECT ON msdb.dbo.sysjobs TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_add_job TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_delete_job TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_add_jobstep TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_update_job TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_add_jobserver TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_add_jobschedule TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_add_category TO VC_ADMIN_ROLE	
GRANT VIEW SERVER STATE TO [vpxuser]	Proporciona acceso a las vistas DMV de SQL Server y a la ejecución de sp_lock.
GRANT VIEW ANY DEFINITION TO [vpxuser]	Necesario para proporcionar al usuario los privilegios para observar los metadatos para objetos de SQL Server.

Tabla 4-6. Permisos de base de datos de Oracle para vCenter Server

Permiso	Descripción
GRANT CONNECT TO VPXADMIN	Necesario para la conexión con la base de datos de Oracle.
GRANT RESOURCE TO VPXADMIN	Necesario para la creación de un activador, secuencia, tipo, procedimiento, etc. De forma predeterminada, el rol RECURSO posee asignados los privilegios CREAR PROCEDIMIENTO, CREAR TABLA y CREAR SECUENCIA. Si el rol RECURSO no posee estos privilegios, concédaselos al usuario de la base de datos de vCenter Server.
GRANT CREATE VIEW TO VPXADMIN	Necesario para crear una vista.
GRANT CREATE SEQUENCE TO VPXADMIN	Necesario para crear una secuencia.
GRANT CREATE TABLE TO VPXADMIN	Necesario para crear una tabla.
GRANT CREATE MATERIALIZED VIEW TO VPXADMIN	Necesario para crear una vista materializada.
GRANT EXECUTE ON dbms_lock TO VPXADMIN	Necesario para garantizar que la base de datos de vCenter Server sea utilizada por una sola instancia de vCenter Server.
GRANT EXECUTE ON dbms_job TO VPXADMIN	Necesario durante la instalación o actualización para la programación y administración de trabajos de SQL. Este permiso no se requiere después de la implementación.
GRANT SELECT ON dba_lock TO VPXADMIN	Necesario para determinar los bloqueos existentes en la base de datos de vCenter Server.
GRANT SELECT ON dba_tablespaces TO VPXADMIN	Necesario durante la actualización para determinar el espacio en disco requerido. Este permiso no se requiere después de la implementación.
GRANT SELECT ON dba_temp_files TO VPXADMIN	Necesario durante la actualización para determinar el espacio en disco requerido. Este permiso no se requiere después de la implementación.
GRANT SELECT ON dba_data_files TO VPXADMIN	Necesario para la supervisión del espacio libre mientras está funcionando vCenter Server.
GRANT SELECT ON v_$session TO VPXADMIN	Vista utilizada para determinar los bloqueos existentes en la base de datos de vCenter Server.
GRANT UNLIMITED TABLESPACE TO VPXADMIN	Necesario para conceder permisos de espacio de tabla ilimitados al usuario de la base de datos de vCenter Server.
GRANT SELECT ON v_$system_event TO VPXADMIN	Necesario para comprobar los cambios del archivo de registro.
GRANT SELECT ON v_$sysmetric_history TO VPXADMIN	Necesario para comprobar la utilización de la CPU.

Tabla 4-6. Permisos de base de datos de Oracle para vCenter Server (continuación)

Permiso	Descripción
GRANT SELECT ON v_$sysstat TO VPXADMIN	Necesario para determinar la frecuencia de aciertos de memoria caché del búfer.
GRANT SELECT ON dba_data_files TO VPXADMIN	Necesario para determinar la utilización del espacio de tabla.
GRANT SELECT ON v_$loghist TO VPXADMIN	Necesario para comprobar la frecuencia del punto de comprobación.

Los privilegios de la base de datos maestra se utilizan para supervisar la base de datos de vCenter Server. Por lo tanto, si se alcanza un umbral determinado, podrá observar una alerta.

Comprobar que vCenter Server puede comunicarse con la base de datos local

Si la base de datos se encuentra en el mismo equipo en el que se va a instalar vCenter Server y se modificó el nombre del equipo, compruebe la configuración. Asegúrese de que el DSN de vCenter Server esté configurado para comunicarse con el nuevo nombre del equipo.

El cambio de nombre del equipo de vCenter Server repercute en la comunicación con la base de datos si el servidor de bases de datos se encuentra en el mismo equipo de vCenter Server. Si modificó el nombre del equipo, puede comprobar que la comunicación permanezca intacta.

Si la base de datos es remota, puede omitir este procedimiento. El cambio de nombre no afecta a la comunicación con las bases de datos remotas.

Después de cambiar el nombre del servidor, compruebe con el administrador o el proveedor de bases de datos que todos los componentes estén en funcionamiento.

Requisitos previos

- Asegúrese de que el servidor de bases de datos se esté ejecutando.
- Asegúrese de que el nombre del equipo vCenter Server esté actualizado en el servicio de nombres de dominio (DNS).

Procedimiento

1 Actualice la información del origen de datos, según sea necesario.

2 Para probar esta condición, puede hacer ping al nombre del equipo.

   Por ejemplo, si el nombre de equipo es `host-1.company.com`, ejecute el siguiente comando en el símbolo del sistema de Windows:

   ```
   ping host-1.company.com
   ```

   Si puede hacer ping al nombre de equipo, el nombre se actualiza en DNS.

Resultados

Se confirma la comunicación con vCenter Server. Puede continuar con la preparación de otros componentes del entorno.

Mantener una base de datos de vCenter Server

Una vez que la instancia de base de datos de vCenter Server y vCenter Server están instalados y funcionan correctamente, realice procesos de mantenimiento de base de datos estándar.

Los procesos de mantenimiento de la base de datos incluyen las siguientes tareas:

- Supervisión del crecimiento del archivo de registro y compactación del archivo de registro de la base de datos, según sea necesario.
- Programación de copias de seguridad regulares de la base de datos.
- Creación de copias de seguridad de la base de datos antes de actualizar vCenter Server.

Consulte la documentación de su proveedor de base de datos para conocer los procedimientos de mantenimiento específicos y obtener asistencia.

Sincronizar los relojes en la red de vSphere

Compruebe que todos los componentes de la red de vSphere tengan sus relojes sincronizados. Si los relojes de las máquinas de la red de vSphere no están sincronizados, los certificados SSL, que están sujetos a limitaciones temporales, pueden no reconocerse como válidos en las comunicaciones entre máquinas de la red.

Los relojes que no están sincronizados pueden ocasionar problemas de autenticación que, a su vez, pueden provocar que la instalación sea incorrecta o evitar que se inicie el servicio vpxd de vCenter Server Appliance.

Verifique que todos los equipos host de Windows en los que se ejecuta vCenter Server estén sincronizados con el servidor de tiempo de red (NTP). Consulte el artículo de la base de conocimientos http://kb.vmware.com/kb/1318.

Para sincronizar los relojes de ESXi con un servidor NTP, puede usar VMware Host Client. Para obtener información sobre cómo editar la configuración de hora de un host ESXi, consulte *Administrar un host único de vSphere*.

Usar una cuenta de usuario para ejecutar vCenter Server

Puede utilizar la cuenta del sistema integrada de Microsoft Windows o una cuenta de usuario para ejecutar vCenter Server. Con una cuenta de usuario, puede habilitar la autenticación de Windows para SQL Server, y esto proporciona más seguridad.

La cuenta de usuario debe ser un administrador en la máquina local. En el asistente de instalación, especifique el nombre de la cuenta como *DomainName**Username*. Deberá configurar la base de datos de SQL Server para permitir el acceso de la cuenta de dominio a SQL Server.

La cuenta del sistema integrada de Microsoft Windows posee más permisos y derechos en el servidor que los que el sistema vCenter Server necesita, lo que podría representar problemas de seguridad.

Importante Si el servicio de vCenter Server se ejecuta en la cuenta del sistema integrada de Microsoft Windows, al utilizar Microsoft SQL Server, vCenter Server solo admite DSN con autenticación de SQL Server.

Para DNS de SQL Server configurados con autenticación de Windows, utilice la misma cuenta de usuario para el servicio VMware VirtualCenter Management Webservices y el usuario de DSN.

Si no tiene pensado utilizar la autenticación de Microsoft Windows para SQL Server o si va a utilizar una base de datos de Oracle, es posible que aún desee configurar una cuenta de usuario local para el sistema vCenter Server. El único requisito es que la cuenta de usuario sea un administrador en la máquina local y la cuenta debe tener concedido el privilegio **Iniciar sesión como servicio**.

Nota A partir de vSphere 6.5, los servicios de vCenter Server no son servicios independientes en Windows SCM, sino que se ejecutan como procesos secundarios del servicio VMware Service Lifecycle Manager.

Instalar vCenter Server en máquinas IPv6

A partir de vSphere 6.5, vCenter Server admite entornos mixtos de IPv4 y IPv6.

Puede conectar vCenter Server con una dirección IPv4 a vCenter Server con una dirección IPv6. Al instalar vCenter Server con una dirección IPv6, use el FQDN o el nombre de host del equipo en el que instala vCenter Server. Al instalar vCenter Server con una dirección IPv4, la práctica recomendada es utilizar el FQDN o el nombre de host del equipo en el que se instala vCenter Server, ya que la dirección IP puede cambiar si se asigna mediante DHCP.

Ejecutar el instalador de vCenter Server desde una unidad de red

Puede ejecutar el instalador de vCenter Server desde una unidad de red, pero no puede instalar el software en una unidad de red.

En Windows, puede ejecutar los instaladores desde la unidad de red e instalar el software en la máquina local.

Información necesaria para instalar vCenter Server o Platform Services Controller en Windows

Al instalar vCenter Server con una instancia integrada de Platform Services Controller, Platform Services Controller o vCenter Server con una instancia externa de Platform Services Controller, el asistente solicita la información de instalación. Se recomienda mantener un registro de los valores introducidos por si debe reinstalar el producto.

Puede utilizar esta hoja de cálculo a fin de registrar la información que necesita para la instalación de vCenter Server con una instancia integrada de Platform Services Controller, Platform Services Controller o vCenter Server con una instancia externa de Platform Services Controller.

Tabla 4-7. Información necesaria para instalar vCenter Server o Platform Services Controller en Windows

Necesario para	Información necesaria	Predeterminado	Su entrada
Todos los tipos de implementación	Nombre del sistema local El nombre de sistema que se va a utilizar para administrar el sistema local. El nombre de sistema debe ser un FQDN. Si no hay un DNS disponible, proporcione una dirección IP estática.	-	
■ vCenter Server con una instancia de Platform Services Controller integrada ■ Platform Services Controller como la primera instancia en un nuevo dominio	Nombre del nuevo dominio de vCenter Single Sign-On	vsphere.local	
	Nombre de usuario	administrador	No puede modificar el nombre de usuario predeterminado durante la instalación.
	Contraseña de la cuenta del administrador de vCenter Single Sign-On La contraseña debe contener al menos 8 caracteres y no más de 20. Esta debe cumplir los siguientes requisitos: ■ Debe contener al menos una letra mayúscula. ■ Debe contener al menos una letra minúscula. ■ Debe contener al menos un número. ■ Debe contener al menos un carácter especial, como una y comercial (&), una almohadilla (#) y el signo de porcentaje (%).	-	
	Nombre del sitio Un nombre para el sitio de vCenter Single Sign-On.	Primer sitio predeterminado	
■ vCenter Server con una instancia de Platform Services Controller externa ■ Platform Services Controller como instancia subsiguiente en un dominio existente	FQDN o dirección IP de la instancia de Platform Services Controller a la que desea unirse Debe unirse a una instancia de Platform Services Controller de la misma versión.	-	
	Puerto HTTPS de la instancia de Platform Services Controller	443	
	Contraseña del usuario administrador de vCenter Single Sign On para el dominio	-	
	Nombre del sitio de vCenter Single Sign-On Puede unirse a un sitio existente o crear uno nuevo.	-	

Tabla 4-7. Información necesaria para instalar vCenter Server o Platform Services Controller en Windows (continuación)

Necesario para	Información necesaria	Predeterminado	Su entrada
■ vCenter Server con una instancia de Platform Services Controller integrada ■ vCenter Server con una instancia de Platform Services Controller externa	Información de la cuenta del servicio de vCenter Server Puede ser la cuenta del sistema local de Windows o una cuenta de servicio del usuario. **Nota** A partir de vSphere 6.5, los servicios de vCenter Server se ejecutan como procesos secundarios del servicio VMware Service Lifecycle Manager.	Cuenta del sistema local de Windows	
	Nombre de usuario de la cuenta Solo si utiliza una cuenta de servicio de usuario.	-	
	Contraseña de la cuenta Solo si utiliza una cuenta de servicio de usuario.	-	
■ vCenter Server con una instancia de Platform Services Controller integrada ■ vCenter Server con una instancia de Platform Services Controller externa	Base de datos de vCenter Server Puede ser la base de datos de VMware Postgres integrada o una base de datos externa existente.	Base de datos de Postgres integrada	
	Nombre de origen de datos (DSN) Solo si utiliza una base de datos externa existente. No se admiten los espacios iniciales y finales. Elimine los espacios al principio y al final del DSN.	-	
	Nombre de usuario de la base de datos Solo si utiliza una base de datos externa existente. No se admiten caracteres que no sean de ASCII.	-	
	Contraseña de base de datos Solo si utiliza una base de datos externa existente.	-	
Todos los tipos de implementación	Puerto HTTP	80	
	Puerto HTTPS	443	
	Puerto de servicio de Syslog	514	
	Puerto TLS de servicio de Syslog	1514	
■ vCenter Server con una instancia de Platform Services Controller integrada ■ Platform Services Controller	Puerto del servicio de token seguro	7444	
■ vCenter Server con una instancia de Platform Services Controller integrada	Puerto de administración de Auto Deploy	6502	
	Puerto de servicio de Auto Deploy	6501	
	puerto de ESXi Dump Collector	6500	
	puerto de latido de ESXi	902	

Tabla 4-7. Información necesaria para instalar vCenter Server o Platform Services Controller en Windows (continuación)

Necesario para	Información necesaria	Predeterminado	Su entrada
■ vCenter Server con una instancia de Platform Services Controller externa	Puerto de vSphere Web Client	9443	
Todos los tipos de implementación	carpeta de destino ■ La carpeta en la que desea instalar vCenter Server o Platform Services Controller. ■ La carpeta en la que desea almacenar los datos de vCenter Server o Platform Services Controller. Las rutas de instalación no pueden contener caracteres que no sean ASCII, comas (,), puntos (.), signos de exclamación (!), numerales (#), arrobas (@) ni signos de porcentaje (%).	■ La carpeta de instalación predeterminada es `C:\Archivos de programa\VMware`. ■ La carpeta predeterminada para almacenamiento de datos es `C:\ProgramData\VMware`.	
■ vCenter Server con una instancia de Platform Services Controller integrada ■ Platform Services Controller	Decida si desea unirse al Programa de mejora de la experiencia del cliente (Customer Experience Improvement Program, CEIP) de VMware Para obtener más información sobre el CEIP, consulte la sección Configurar el Programa de mejora de la experiencia del cliente en *Administrar vCenter Server y hosts*.	Unirse al CEIP	

Instalar vCenter Server y Platform Services Controller en Windows

Puede instalar vCenter Server con una instancia integrada de Platform Services Controller, Platform Services Controller o vCenter Server con una instancia externa de Platform Services Controller en un equipo Windows físico o virtual.

Debe descargar el archivo ISO del instalador de vCenter Server, montarlo en el equipo host Windows donde desea realizar la instalación, iniciar el asistente de instalación y proporcionar las entradas requeridas para la instalación y la configuración.

Antes de instalar la instancia de vCenter Server que utiliza una base de datos externa, debe preparar la base de datos. Consulte Preparar las bases de datos de vCenter Server para la instalación.

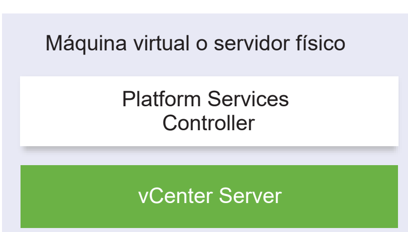
Importante Para usar topologías con instancias externas de Platform Services Controller, es necesario instalar las instancias de replicación de Platform Services Controller en secuencia. Después de implementar correctamente todas las instancias de Platform Services Controller en el dominio, se pueden realizar instalaciones simultáneas de varias instancias de vCenter Server que apuntan a una instancia externa común de Platform Services Controller.

Instalar vCenter Server con una instancia integrada de Platform Services Controller en Windows

Puede implementar vCenter Server, los componentes de vCenter Server y Platform Services Controller en una máquina virtual o servidor físico.

Después de implementar vCenter Server con una instancia de Platform Services Controller integrada, puede volver a configurar la topología y cambiar a vCenter Server con una instancia de Platform Services Controller externa. Este es un proceso unidireccional. Una vez realizado, no se puede volver a vCenter Server con una instancia de Platform Services Controller integrada. Puede redireccionar la instancia de vCenter Server solo a una instancia de Platform Services Controller externa configurada para replicar los datos de infraestructura dentro del mismo dominio.

Figura 4-1. vCenter Server con una instancia de Platform Services Controller integrada



Requisitos previos

- Compruebe que su sistema cumpla con los requisitos mínimos de hardware y software. Consulte Requisitos de vCenter Server para Windows.
- Descargar el instalador de vCenter Server para Windows.
- Si desea utilizar vSphere Web Client en el equipo host en el que va a instalar vCenter Server, compruebe que Adobe Flash Player 11.9 o posterior esté instalado en el sistema.

Procedimiento

1 En el directorio del instalador del software, haga doble clic en el archivo `autorun.exe` para iniciar el instalador.

2 Seleccione **vCenter Server para Windows** y haga clic en **Instalar**.

3 Siga las indicaciones del asistente para instalación para revisar la página principal y acepte el contrato de licencia.

4 Seleccione **vCenter Server y Platform Services Controller** integrado y haga clic en **Siguiente**.

5 Introduzca el nombre de la red del sistema, de preferencia un FQDN y haga clic en **Siguiente**.

También puede introducir una dirección IP. Si introduce una dirección IP, proporcione una dirección IP estática.

Importante Asegúrese de que la FQDN o la dirección IP que proporciona no cambie. El nombre del sistema no puede cambiar después de la implementación. Si el nombre del sistema cambia, debe desinstalar vCenter Server y volver a instalarlo.

---

6 Configure el nuevo dominio de vCenter Single Sign-On y haga clic en **Siguiente**.

a Introduzca el nombre de dominio; por ejemplo, **`vsphere.local`**.

b Defina la contraseña para la cuenta de administrador de vCenter Single Sign-On.

Esta es la contraseña del usuario administrator@*su_ nombre_ de_ dominio*. Tras la instalación, puede iniciar sesión en vCenter Single Sign-On y en vCenter Server como administrator@*su_ nombre_ de_ dominio*.

c Introduzca el nombre del sitio para vCenter Single Sign-On.

El nombre del sitio es importante si utiliza vCenter Single Sign-On en varias ubicaciones. El nombre del sitio debe contener caracteres alfanuméricos. Seleccione su propio nombre para el sitio de vCenter Single Sign-On. No puede cambiar el nombre después de la instalación.

En los nombres de sitio no se admiten caracteres ASCII extendidos ni caracteres que no sean ASCII. Igualmente, deben incluir caracteres alfanuméricos y coma (,), punto (.), signo de interrogación (?), guion (-), guion bajo (_), signo más (+) o signo igual (=).

7 Seleccione la cuenta de servicio de vCenter Server y haga clic en **Siguiente**.

Nota A partir de vSphere 6.5, los servicios de vCenter Server no son servicios independientes en Windows SCM, sino que se ejecutan como procesos secundarios del servicio VMware Service Lifecycle Manager.

Opción	Descripción
Utilizar cuenta del sistema local Windows	El servicio vCenter Server se ejecuta en la cuenta del sistema local Windows. Esta opción le impide conectarse a una base de datos externa mediante la autenticación integrada de Windows.
Especificar una cuenta de servicio de usuario	El servicio vCenter Server se ejecuta en una cuenta de usuario administrativo con el nombre de usuario y la contraseña que proporcione. **Importante** Las credenciales de usuario que brinda deben pertenecer a un usuario del grupo de administradores locales y tener el privilegio **Inicio de sesión como servicio**.

8 Seleccione el tipo de base de datos que desee utilizar y haga clic en **Siguiente**.

Opción	Descripción
Usar una base de datos integrada (PostgreSQL)	vCenter Server utiliza la base de datos integrada de PostgreSQL. Esta base de datos es adecuada para implementaciones de pequeña escala.
Usar una base de datos externa	vCenter Server utiliza una base de datos externa existente. a Seleccione la base de datos en la lista de DSN disponibles. b Escriba el nombre de usuario y la contraseña del DSN. Si su base de datos utiliza autenticación de Windows NT, los cuadros de texto para nombre de usuario y contraseña están deshabilitados.

9 Para cada componente, acepte los números de puerto predeterminados o, si otro servicio está utilizando los valores predeterminados, introduzca los puertos alternativos y haga clic en **Siguiente**.

Asegúrese de que los puertos 80 y 443 estén libres y sean dedicados, para que vCenter Single Sign-On pueda utilizarlos. De lo contrario, utilice puertos personalizados durante la instalación.

10 (opcional) Cambie las carpetas de destino predeterminadas y haga clic en **Siguiente**.

Importante No utilice carpetas que terminen con un signo de exclamación (!).

11 Revise la página del Programa de mejora de la experiencia del cliente (Customer Experience Improvement Program, CEIP) de VMware y decida si desea unirse a él.

Para obtener más información sobre el CEIP, consulte la sección Configurar el Programa de mejora de la experiencia del cliente en *Administrar vCenter Server y hosts*.

12 Haga clic en **Siguiente**.

13 Revise el resumen de la configuración de instalación y haga clic en **Instalar** para iniciar la instalación.

14 (opcional) Cuando finalice la instalación, haga clic en **Iniciar vSphere Web Client** para abrir vSphere Web Client e inicie sesión en vCenter Server.

15 Haga clic en **Finalizar** para cerrar el instalador.

Resultados

vCenter Server, los componentes devCenter Server y Platform Services Controller están instalados.

Instalar Platform Services Controller en Windows

Antes de instalar vCenter Server con una instancia externa de Platform Services Controller, debe instalar Platform Services Controller. Platform Services Controller contiene los servicios comunes, como vCenter Single Sign-On y License service, que se pueden compartir en varias instancias de vCenter Server.

Puede instalar varias instancias de Platform Services Controller de la misma versión y asociarlas como partners de replicación al mismo dominio de vCenter Single Sign-On. No se admiten instalaciones simultáneas de replicación de instancias de Platform Services Controller. Deberá instalar las instancias de Platform Services Controller en el dominio en secuencia.

Importante Si desea reemplazar el certificado firmado por VMCA por un certificado firmado por CA, instale Platform Services Controller en primer lugar y, a continuación, incluya VMCA en la cadena de certificados y genere certificados nuevos desde VMCA que estén firmados por toda la cadena. A continuación, puede instalar vCenter Server. Para obtener información sobre cómo administrar certificados de vCenter Server, consulte *Administrar Platform Services Controller*.

Requisitos previos

- Compruebe que su sistema cumpla con los requisitos mínimos de hardware y software. Consulte Requisitos de vCenter Server para Windows.
- Descargar el instalador de vCenter Server para Windows.

Procedimiento

1 En el directorio del instalador del software, haga doble clic en el archivo `autorun.exe` para iniciar el instalador.

2 Seleccione **vCenter Server para Windows** y haga clic en **Instalar**.

3 Siga las indicaciones del asistente para instalación para revisar la página principal y acepte el contrato de licencia.

4 Seleccione **Platform Services Controller** y haga clic en **Siguiente**.

5 Introduzca el nombre del sistema, preferiblemente un FQDN, y haga clic en **Siguiente**.

También puede introducir una dirección IP. Si introduce una dirección IP, proporcione una dirección IP estática.

Importante Cuando proporcione un FQDN o una dirección IP como el nombre del sistema de Platform Services Controller, asegúrese de que el FQDN o la dirección IP no sufran cambios. Si el FQDN o la dirección IP del equipo host cambia, deberá volver a instalar Platform Services Controller y las instancias de vCenter Server registradas con este. El FQDN o la dirección IP de Platform Services Controller se utiliza para generar un certificado SSL para el equipo host de Platform Services Controller.

6 Cree un nuevo dominio de vCenter Single Sign-On o únase a un dominio existente.

Opción	Descripción
Crear un nuevo dominio de Single Sign-On	Crea un nuevo dominio de vCenter Single Sign-On. a Introduzca el nombre de dominio; por ejemplo, **`vsphere.local`**. b Establezca el nombre de usuario de la cuenta de administrador de vCenter Single Sign-On, por ejemplo, **`administrator`**. Después de la implementación, puede iniciar sesión en vCenter Single Sign-On y en vCenter Server como *adminstrator_user_name@su_nombre_de_dominio*. c Defina la contraseña para la cuenta de administrador de vCenter Single Sign-On. Esta es la contraseña del usuario *adminstrator_user_name@su_nombre_de_dominio*. d Introduzca el nombre del sitio para vCenter Single Sign-On. El nombre del sitio es importante si utiliza vCenter Single Sign-On en varias ubicaciones. El nombre del sitio debe contener caracteres alfanuméricos. Seleccione su propio nombre para el sitio de vCenter Single Sign-On. No puede cambiar el nombre después de la instalación. En los nombres de sitio no se admiten caracteres ASCII extendidos ni caracteres que no sean ASCII. Igualmente, deben incluir caracteres alfanuméricos y coma (,), punto (.), signo de interrogación (?), guion (-), guion bajo (_), signo más (+) o signo igual (=). **Nota** Al configurar una instancia de Embedded Linked Mode, utilice **`Primer sitio predeterminado`** como el nombre del sitio para la primera instancia. e Haga clic en **Siguiente**.
Unirse a un dominio de vCenter Single Sign-On existente	Se une a un nuevo servidor vCenter Single Sign-On a un dominio de vCenter Single Sign-On en una instancia de Platform Services Controller existente. Debe proporcionar la información sobre el servidor vCenter Single Sign-On al que se va a unir el nuevo servidor vCenter Single Sign-On. a Escriba el nombre de dominio completo (fully qualified domain name, FQDN) o la dirección IP de la instancia de Platform Services Controller que contiene el servidor vCenter Single Sign-On al que se va a unir. b Introduzca el puerto HTTPS que se usará para la comunicación con Platform Services Controller. c Escriba el nombre de usuario y la contraseña de la cuenta de administrador de vCenter Single Sign-On. d Haga clic en **Siguiente**. e Apruebe el certificado que brinda el equipo remoto y determine si desea crear un sitio de vCenter Single Sign-On o unirse a uno existente. f Determine si desea crear un sitio de vCenter Single Sign-On o unirse a uno existente.

7 Haga clic en **Siguiente**.

8 Para cada componente, acepte los números de puerto predeterminados o, si otro servicio está utilizando los valores predeterminados, introduzca los puertos alternativos y haga clic en **Siguiente**.

   Asegúrese de que los puertos 80 y 443 estén libres y sean dedicados, para que vCenter Single Sign-On pueda utilizarlos. De lo contrario, utilice puertos personalizados durante la instalación.

9 (opcional) Cambie las carpetas de destino predeterminadas y haga clic en **Siguiente**.

   Importante No utilice carpetas que terminen con un signo de exclamación (!).

10 Revise la página del Programa de mejora de la experiencia del cliente (Customer Experience Improvement Program, CEIP) de VMware y decida si desea unirse a él.

   Para obtener más información sobre el CEIP, consulte la sección Configurar el Programa de mejora de la experiencia del cliente en *Administrar vCenter Server y hosts*.

11 Revise el resumen de la configuración de instalación y haga clic en **Instalar** para iniciar la instalación.

12 Una vez finalizada la instalación, haga clic en **Finalizar** para cerrar el instalador.

Resultados

Platform Services Controller está instalado.

Pasos siguientes

Instale vCenter Server en otra máquina virtual o servidor físico con Windows y registre vCenter Server y los componentes de vCenter Server en Platform Services Controller.

Instalar vCenter Server con una instancia externa de Platform Services Controller en Windows

Después de instalar Platform Services Controller en un equipo host con Windows o de implementar un dispositivo Platform Services Controller, podrá instalar vCenter Server y los componentes de vCenter Server y conectar la instancia de vCenter Server al Platform Services Controller implementado.

Requisitos previos

- Compruebe que su sistema cumpla con los requisitos mínimos de hardware y software. Consulte Requisitos de vCenter Server para Windows.
- Descargar el instalador de vCenter Server para Windows.
- Si desea utilizar vSphere Web Client en el equipo host en el que va a instalar vCenter Server, compruebe que Adobe Flash Player 11.9 o posterior esté instalado en el sistema.

Procedimiento

1 En el directorio del instalador del software, haga doble clic en el archivo `autorun.exe` para iniciar el instalador.

2 Seleccione **vCenter Server para Windows** y haga clic en **Instalar**.

3 Siga las indicaciones del asistente para instalación para revisar la página principal y acepte el contrato de licencia.

4 Seleccione **vCenter Server** y haga clic en **Siguiente**.

5 Introduzca el nombre de red del sistema, preferiblemente una dirección IP estática, y haga clic en **Siguiente**.

Importante El nombre que introduzca se codifica en el certificado SSL del sistema. Los componentes se comunican entre sí con este nombre. El nombre del sistema debe ser una dirección IP estática o un nombre de dominio completo (FQDN). Asegúrese de que no se cambie el nombre del sistema. No podrá cambiar el nombre del sistema después de que se complete la instalación.

6 Proporcione el nombre del sistema de Platform Services Controller que ya ha instalado o implementado, el puerto HTTPS que se va a utilizar para la comunicación con el servidor de vCenter Single Sign-On y la contraseña de vCenter Single Sign-On, y haga clic en **Siguiente**.

Importante Asegúrese de utilizar la dirección IP o el FQDN que proporcionó durante la instalación de Platform Services Controller. Si ha proporcionado el FQDN como un nombre del sistema de Platform Services Controller, no podrá utilizar una dirección IP y a la inversa. Cuando un servicio de vCenter Server se conecta a un servicio que se ejecuta en Platform Services Controller, se verifica el certificado. Si cambia la dirección IP o el FQDN, se produce un error en la verificación y vCenter Server no puede conectarse al Platform Services Controller.

7 Apruebe el certificado proporcionado por la máquina remota.

8 Seleccione la cuenta de servicio de vCenter Server y haga clic en **Siguiente**.

Nota A partir de vSphere 6.5, los servicios de vCenter Server no son servicios independientes en Windows SCM, sino que se ejecutan como procesos secundarios del servicio VMware Service Lifecycle Manager.

Opción	Descripción
Utilizar cuenta del sistema local Windows	El servicio vCenter Server se ejecuta en la cuenta del sistema local Windows. Esta opción le impide conectarse a una base de datos externa mediante la autenticación integrada de Windows.
Especificar una cuenta de servicio de usuario	El servicio vCenter Server se ejecuta en una cuenta de usuario administrativo con el nombre de usuario y la contraseña que proporcione. **Importante** Las credenciales de usuario que brinda deben pertenecer a un usuario del grupo de administradores locales y tener el privilegio **Inicio de sesión como servicio**.

9 Seleccione el tipo de base de datos que desee utilizar y haga clic en **Siguiente**.

Opción	Descripción
Usar una base de datos integrada (PostgreSQL)	vCenter Server utiliza la base de datos integrada de PostgreSQL. Esta base de datos es adecuada para implementaciones de pequeña escala.
Usar una base de datos externa	vCenter Server utiliza una base de datos externa existente. a Seleccione la base de datos en la lista de DSN disponibles. b Escriba el nombre de usuario y la contraseña del DSN. Si su base de datos utiliza autenticación de Windows NT, los cuadros de texto para nombre de usuario y contraseña están deshabilitados.

10 Para cada componente, acepte los números de puerto predeterminados o, si otro servicio está utilizando los valores predeterminados, introduzca los puertos alternativos y haga clic en **Siguiente**.

11 (opcional) Cambie las carpetas de destino predeterminadas y haga clic en **Siguiente**.

Importante No utilice carpetas que terminen con un signo de exclamación (!).

12 Revise el resumen de la configuración de instalación y haga clic en **Instalar** para iniciar la instalación.

13 (opcional) Cuando finalice la instalación, haga clic en **Iniciar vSphere Web Client** para abrir vSphere Web Client e inicie sesión en vCenter Server.

14 Haga clic en **Finalizar** para cerrar el instalador.

Resultados

vCenter Server se instala en modo de evaluación. Puede activar vCenter Server mediante vSphere Web Client. Para obtener información sobre la activación de vCenter Server, consulte *Administrar vCenter Server y hosts*.

Instalar vCenter Server en un entorno con varias NIC en Windows

Si desea instalar vCenter Server con una instancia de Platform Services Controller externa en un entorno con varias NIC, debe mantener un registro de las direcciones IP o los FQDN que utiliza como nombres de red del sistema.

Por ejemplo, si desea instalar Platform Services Controller en una máquina virtual y vCenter Server en otra, y cada máquina virtual tiene dos NIC, puede usar el siguiente flujo de trabajo:

1 Instale Platform Services Controller en una de las máquinas virtuales y utilice una de sus direcciones IP o un FQDN como nombre de red del sistema.

2 En la otra máquina virtual, inicie la instalación de vCenter Server y use una de sus direcciones IP o un FQDN como nombre de red del sistema.

3 Cuando se le pida que proporcione el nombre de red del sistema de Platform Services Controller, escriba la dirección IP o el FQDN que introdujo durante la instalación de Platform Services Controller.

   Si escribe la otra dirección IP o el otro FQDN de Platform Services Controller, recibirá un mensaje de error.

4 Una vez que finalice la instalación, podrá iniciar sesión en vSphere Web Client con cualquier dirección IP o FQDN de NIC de vCenter Server.

Después de instalar vCenter Server o implementar vCenter Server Appliance

5

Después de instalar vCenter Server o implementar vCenter Server Appliance, tenga en cuenta estas opciones posteriores a la instalación antes de agregarle inventario a vCenter Server para que lo administre.

Para obtener información sobre cómo configurar el servicio vSphere Authentication Proxy, consulte *vSphere Security*.

Este capítulo incluye los siguientes temas:

Iniciar sesión en vCenter Server con vSphere Web Client

Inicie sesión en vCenter Server con vSphere Web Client para administrar su inventario de vSphere.

En vSphere 6.0 y versiones posteriores, vSphere Web Client se instala como parte de vCenter Server en Windows o la implementación de vCenter Server Appliance. De esta manera, vSphere Web Client siempre apunta a la misma instancia de vCenter Single Sign-On.

Procedimiento

1 Abra el explorador web e introduzca la URL de vSphere Web Client: **https://*vcenter_server_ip_address_or_fqdn*/vsphere-client**.

2 Introduzca las credenciales de un usuario que tenga permisos en vCenter Server y haga clic en **Iniciar sesión**.

3 Si aparece un mensaje de advertencia acerca de un certificado SSL que no es de confianza, seleccione la acción correcta según su directiva de seguridad.

Opción	Acción
Omita la advertencia de seguridad para esta sesión de inicio de sesión solamente.	Haga clic en **Omitir**.
Omita la advertencia de seguridad para esta sesión de inicio de sesión e instale el certificado predeterminado para que la advertencia no vuelva a aparecer.	Seleccione **Instalar este certificado y no mostrar ninguna advertencia de seguridad para este servidor** y haga clic en **Omitir**. Seleccione esta opción solamente si al usar el certificado predeterminado no se presenta un problema de seguridad en el entorno.
Cancele e instale un certificado firmado antes de continuar.	Haga clic en **Cancelar** y asegúrese de que esté instalado un certificado firmado en el sistema de vCenter Server antes de intentar volver a conectarse.

Resultados

vSphere Web Client conecta todos los sistemas devCenter Server para los que el usuario especificado tiene permisos, y así permite ver y administrar el inventario.

Instalar el complemento de autenticación mejorado de VMware

El complemento de autenticación mejorado de VMware ofrece autenticación integrada en Windows y funcionalidad de tarjeta inteligente basada en Windows.

En esta versión de vSphere 6.5, el complemento de autenticación mejorado de VMware reemplaza al complemento de integración de clientes a partir de vSphere 6.0 y versiones anteriores. El complemento de autenticación mejorado ofrece autenticación integrada en Windows y funcionalidad de tarjeta inteligente basada en Windows. Estas son las únicas dos funciones que se transfirieron del anterior complemento de integración de clientes. El complemento de autenticación mejorado puede funcionar sin problemas si ya tiene el complemento de integración de clientes instalado en el sistema de vSphere 6.0 o una versión anterior. No hay ningún conflicto si ambos complementos están instalados.

Mire el video “vSphere Web Client después de la eliminación del complemento de integración de clientes” para obtener más información sobre los cambios del flujo de trabajo en vSphere Client:

vSphere Web Client después de la eliminación del complemento de integración de clientes
(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_6bib1xjv/uiConfId/49694343/)

Instale el complemento solo una vez solo una vez para habilitar todas las funcionalidades que proporciona.

Para obtener información sobre los exploradores y los sistemas operativos compatibles, consulte la documentación de *Instalar y configurar vSphere*.

Procedimiento

1 Abra un explorador web y escriba la URL de vSphere Web Client.

2 En la parte inferior de la página de inicio de sesión de vSphere Web Client, haga clic en **Descargar complemento de autenticación mejorado**.

3 Si el navegador bloquea la instalación mediante la emisión de errores de certificado o la ejecución de un bloqueador de elementos emergentes, siga las instrucciones de la Ayuda para solucionar el problema.

4 Guarde el complemento en el equipo y ejecute el archivo ejecutable.

5 Ingrese en el asistente de instalación del complemento de autenticación mejorado de VMware y del servicio de complementos de VMware que se ejecutan en forma sucesiva.

6 Cuando finalicen las instalaciones, actualice el explorador.

7 En el cuadro de diálogo Solicitud de protocolo externo, haga clic en **Iniciar aplicación** para ejecutar el complemento de autenticación mejorado.

   El vínculo para descargar el complemento desaparece de la página de inicio de sesión.

Recopilar archivos de registro de vCenter Server

Después de instalar vCenter Server, puede recopilar los archivos de registro de vCenter Server para el diagnóstico y la solución de problemas.

Nota Este procedimiento brinda información sobre cómo recopilar los archivos de registro para la instalación de Windows de vCenter Server. Para obtener información sobre cómo exportar un paquete de soporte y examinar los archivos de registro en vCenter Server Appliance, consulte *Configurar vCenter Server Appliance*.

Procedimiento

1 Inicie sesión como administrador en la máquina con Windows en la que está instalado vCenter Server.

2 Desplácese hasta **Inicio > Programas > VMware > Generar el paquete de registros de vCenter Server** para generar el paquete de registros.

   Puede generar paquetes de registros de vCenter Server incluso si no puede conectar con vCenter Server a través de vSphere Web Client.

Resultados

Los archivos de registro para el sistema vCenter Server se generan y se almacenan en un archivo `.tgz` en su escritorio.

Redirigir vCenter Server a otra instancia de Platform Services Controller externa

La unión de las instancias de Platform Services Controller externas en el mismo dominio de vCenter Single Sign-On garantiza la alta disponibilidad del sistema.

Si una instancia externa de Platform Services Controller deja de responder o si se desea distribuir la carga de una instancia externa de Platform Services Controller, es posible volver a apuntar las instancias de vCenter Server a otra instancia de Platform Services Controller dentro del mismo dominio y sitio.

- Puede redirigir la instancia de vCenter Server a una instancia de Platform Services Controller funcional existente que tenga la capacidad de carga libre en el mismo dominio y el mismo sitio.
- Puede instalar o implementar una nueva instancia de Platform Services Controller en el mismo dominio y el mismo sitio a los que redirigirá la instancia vCenter Server.

Requisitos previos

- Si la instancia de Platform Services Controller antigua no responde, quite el nodo y limpie los datos obsoletos de vmdir mediante la ejecución del comando `cmsso-util unregister`. Para obtener información sobre la retirada de una instancia de Platform Services Controller, consulte https://kb.vmware.com/kb/2106736.
- Compruebe que la instancia antigua y la nueva de Platform Services Controller estén en el mismo dominio y sitio de vCenter Single Sign-On mediante la ejecución del comando `vdcrepadmin -f showservers`. Para obtener información sobre el uso del comando, consulte https://kb.vmware.com/kb/2127057.
- Si desea redirigir una instancia de vCenter Server Appliance que se configuró en un clúster de vCenter HA, elimine la configuración de vCenter HA. Para obtener información sobre la forma de eliminar una configuración de vCenter HA, consulte *Disponibilidad de vSphere*.

Procedimiento

1 Inicie sesión en la instancia de vCenter Server.

   - Para una instancia de vCenter Server Appliance, inicie sesión en el shell de vCenter Server Appliance como raíz.
   - Para una instancia de vCenter Server en Windows, inicie sesión como administrador en la máquina virtual o el servidor físico de vCenter Server.

2 Si la instancia de vCenter Server se ejecuta en Windows, abra el símbolo del sistema de este sistema operativo y desplácese hasta `C:\Archivos de programa\VMware\vCenter Server\bin`.

3 Ejecute el comando `cmsso-util repoint`.

```
cmsso-util repoint --repoint-psc psc_fqdn_or_static_ip [--dc-port port_number]
```

donde los corchetes ([]) encierran las opciones del comando.

Aquí, *psc_fqdn_or_static_ip* es el nombre de sistema utilizado para identificar la instancia de Platform Services Controller. El nombre de este sistema debe ser un FQDN o una dirección IP estática.

Nota El valor de FQDN distingue entre mayúsculas y minúsculas.

Utilice la opción `--dc-port port_number` si la instancia de Platform Services Controller se ejecuta en un puerto HTTPS personalizado. El valor predeterminado del puerto HTTPS es 443.

4 Inicie sesión en la instancia de vCenter Server mediante vSphere Web Client para comprobar que la instancia de vCenter Server esté en ejecución y pueda administrarse.

Resultados

La instancia de vCenter Server está registrada con la nueva instancia de Platform Services Controller.

Pasos siguientes

Si redirigió una instancia de vCenter Server Appliance que se configuró en un clúster de vCenter HA, puede volver a configurar el clúster de vCenter HA. Para obtener información sobre la forma de configurar vCenter HA, consulte *Disponibilidad de vSphere*.

Reconfigurar una instancia de vCenter Server independiente con una instancia de Platform Services Controller integrada en un vCenter Server con una instancia de Platform Services Controller externa

Si implementó o instaló una instancia de vCenter Server independiente con una instancia de Platform Services Controller integrada y desea ampliar el dominio de vCenter Single Sign-On con más instancias de vCenter Server, puede reconfigurar y redireccionar la instancia de vCenter Server existente a una instancia de Platform Services Controller externa.

Figura 5-1. Reconfiguración de una instancia de vCenter Server independiente con una instancia de Platform Services Controller integrada y redireccionamiento a una instancia de Platform Services Controller externa

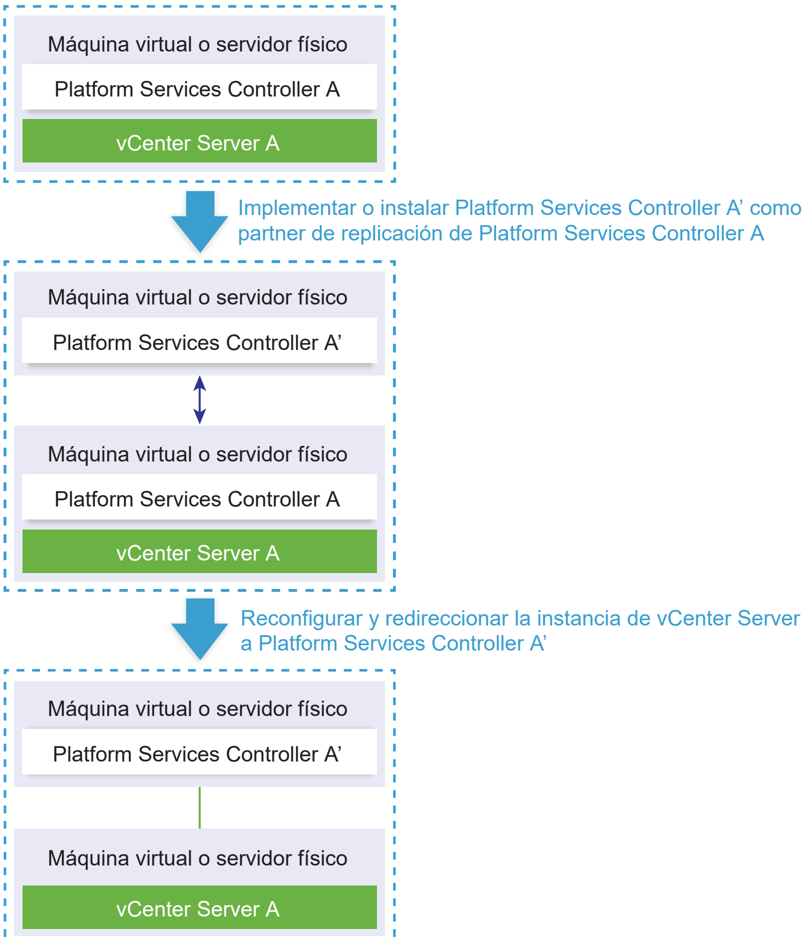


Tabla 5-1. Leyenda

Flecha o línea	Descripción
	Acuerdo de replicación entre dos instancias de Platform Services Controller
	Registro de vCenter Server en una instancia de Platform Services Controller externa
	Paso de transición

Nota La reconfiguración de una instancia de vCenter Server con una instancia de Platform Services Controller integrada y el redireccionamiento a una instancia de Platform Services Controller externa es un proceso de un solo sentido después del cual no se puede volver a cambiar a vCenter Server con una instancia de Platform Services Controller integrada.

Requisitos previos

- Implemente o instale la instancia de Platform Services Controller externa como partner de replicación de la instancia de Platform Services Controller integrada existente en el mismo sitio de vCenter Single Sign-On.

  Nota Puede determinar el sitio de vCenter Single Sign-On actual mediante el comando `vmfad-cli`.

  - En el caso de una instancia de vCenter Server Appliance con una instancia de Platform Services Controller integrada, inicie sesión en el shell del dispositivo como raíz y ejecute el comando.

    ```
    /usr/lib/vmware-vmafd/bin/vmafd-cli get-site-name --server-name localhost
    ```

  - Para una instalación de Windows de una instancia de vCenter Server con una instancia de Platform Services Controller integrada, inicie sesión en el equipo Windows como administrador, abra el símbolo del sistema de Windows y ejecute el comando.

    ```
    C:\Program Files\VMware\vCenter Server\vmafdd\vmafd-cli get-site-name --server-name
    localhost
    ```

- Cree snapshots de vCenter Server con una instancia de Platform Services Controller integrada y una instancia de Platform Services Controller externa, de manera que pueda revertir a los snapshots si la reconfiguración produce errores.
- Si desea volver a configurar vCenter Server Appliance con una instancia integrada de Platform Services Controller que se configuró en un clúster de vCenter HA, elimine la configuración de vCenter HA. Para obtener información sobre la forma de eliminar una configuración de vCenter HA, consulte *Disponibilidad de vSphere*.

Procedimiento

1 Inicie sesión en la instancia de vCenter Server con una instancia de Platform Services Controller integrada.

Opción	Pasos
Para un vCenter Server Appliance con una instancia de Platform Services Controller integrada	Inicie sesión en el shell del dispositivo como raíz. ■ Si tiene acceso directo a la consola del dispositivo, presione Alt+F1. ■ Si desea conectarse de forma remota, utilice SSH u otra conexión de consola remota para iniciar una sesión en el dispositivo.
Para una instalación de Windows de vCenter Server con una instancia de Platform Services Controller integrada	Inicie sesión en el equipo Windows como administrador, abra el símbolo del sistema de Windows y desplácese hasta `C:\Archivos de programa\VMware\vCenter Server\bin`.

2 Compruebe que todos los servicios de Platform Services Controller estén en ejecución.

Ejecute el comando `service-control --status --all`.

Los servicios de Platform Services Controller que deben ejecutarse son VMware License Service, VMware Identity Management Service, VMware Security Token Service, VMware Certificate Service y VMware Directory Service.

3 Ejecute el comando `cmsso-util reconfigure`.

```
cmsso-util reconfigure --repoint-psc psc_fqdn_or_static_ip --username username --domain-name domain_name --passwd password [--dc-port port_number]
```

donde los corchetes [ ] encierran elementos opcionales.

Aquí, *psc_ fqdn_ or_ static_ ip* representa el nombre del sistema utilizado para identificar la instancia de Platform Services Controller externa. El nombre de este sistema debe ser un FQDN o una dirección IP estática.

Nota El valor de FQDN distingue entre mayúsculas y minúsculas.

Las opciones *username* y *password* son el nombre de usuario y la contraseña del administrador de vCenter Single Sign-On *domain_ name*.

Utilice la opción `--dc-port` si la instancia de Platform Services Controller externa se ejecuta en un puerto HTTPS personalizado. El valor predeterminado del puerto HTTPS es 443.

Por ejemplo, si la instancia de Platform Services Controller externa se ejecuta en un puerto HTTPS 449 personalizado, debe ejecutar:

```
cmsso-util reconfigure --repoint-psc psc.acme.local --username administrator --domain-name vsphere.local --passwd Password1! --dc-port 449
```

4 Inicie sesión en la instancia de vCenter Server mediante vSphere Web Client para comprobar que la instancia de vCenter Server esté en ejecución y pueda administrarse.

Resultados

vCenter Server con una instancia de Platform Services Controller integrada se disminuye de nivel, y vCenter Server se direcciona a una instancia de Platform Services Controller externa.

Pasos siguientes

- Puede implementar o instalar instancias de vCenter Server y Platform Services Controller adicionales en el dominio de vCenter Single Sign-On.
- Si volvió a configurar vCenter Server Appliance con una instancia integrada de Platform Services Controller que se configuró en un clúster de vCenter HA, puede volver a configurar el clúster de vCenter HA. Para obtener información sobre la forma de configurar vCenter HA, consulte *Disponibilidad de vSphere*.

Restaurar vCenter Server Appliance y crear una copia de seguridad de ella con base en archivos

6

vCenter Server Appliance admite un mecanismo de restauración y copia de seguridad basado en archivos que permite recuperar el entorno después de que se produzca un error.

En vSphere 6.5, se puede usar la interfaz de administración de vCenter Server Appliance para crear una copia de seguridad basada en archivos de vCenter Server Appliance y del dispositivo de Platform Services Controller. Después de crear la copia de seguridad, se puede restaurar mediante el instalador de GUI del dispositivo.

La interfaz de administración de vCenter Server Appliance se usa para realizar una copia de seguridad basada en archivos de la configuración de núcleos de vCenter Server, del inventario y de los datos históricos que elija. Los datos incluidos en la copia de seguridad se transmiten mediante FTP, FTPS, HTTP, HTTPS o SCP a un sistema remoto. La copia de seguridad no se almacena en vCenter Server Appliance.

Solo se puede realizar una restauración basada en archivos de una instancia de vCenter Server Appliance para la cual se haya hecho previamente una copia de seguridad mediante la interfaz de administración de vCenter Server Appliance. Puede realizar esta operación de restauración mediante el instalador de GUI de vCenter Server Appliance. El proceso consiste en implementar una nueva instancia de vCenter Server Appliance y en copiar los datos de la copia de seguridad basada en archivos a un nuevo dispositivo.

Importante Si se realiza una copia de seguridad de un clúster de vCenter Server Appliance de alta disponibilidad, la operación de copia de seguridad solo copia la instancia principal de vCenter Server. Antes de restaurar un clúster de vCenter Server Appliance de alta disponibilidad, debe apagar los nodos activo, pasivo y testigo. La operación de restauración restaura la instancia de vCenter Server en el modo de vCenter Server sin alta disponibilidad. Una vez finalizada correctamente la operación de restauración, debe reconstruir el clúster.

Este capítulo incluye los siguientes temas:

- Consideraciones y limitaciones para la restauración y la copia de seguridad basada en archivos
- Realizar una copia de seguridad de vCenter Server Appliance mediante la interfaz de administración de vCenter Server Appliance

- Restaurar una instancia de vCenter Server Appliance desde una copia de seguridad basada en archivos

Consideraciones y limitaciones para la restauración y la copia de seguridad basada en archivos

Al realizar una operación de copia de seguridad o restauración de un entorno de vCenter Server, tenga en cuenta estas consideraciones y limitaciones.

Protocolos

Las siguientes consideraciones se aplican a los protocolos de restauración y copia de seguridad basada en archivos:

- FTP y HTTP no son protocolos seguros.
- Los servidores de copia de seguridad deben admitir al menos 10 conexiones simultáneas por cada vCenter Server Appliance.
- Es necesario tener permisos de escritura para la carga y permisos de lectura para la descarga.
- Solo el modo explícito es compatible con FTPS.
- Si se usa HTTP o HTTPS, es necesario habilitar WebDAV en el servidor web de copia de seguridad.
- Solo se pueden usar FTP, FTPS, HTTP o HTTPS para transmitir datos a través de un servidor proxy HTTP.
- Es posible usar direcciones URL IPv4 e IPv6 en las operaciones de restauración y copia de seguridad basada en archivos de vCenter Server Appliance. No se admite el modo mixto de versiones de IP entre el servidor de copia de seguridad y vCenter Server Appliance.
- Si utiliza el protocolo SCP, debe utilizar el servidor de copia de seguridad de Linux.

Configuración

Después de una restauración, las siguientes configuraciones se revierten al estado que tenían cuando se realizó la copia de seguridad.

- Configuración de recursos de máquinas virtuales
- Jerarquía y configuración del grupo de recursos
- Pertenencia de clúster-host
- Reglas y configuración de DRS

Storage DRS

Si se modifica la configuración, es posible que las siguientes opciones cambien después de una restauración.

- Configuración del clúster de almacén de datos
- Pertenencia del clúster de almacén de datos
- Opciones de administración de recursos de E/S del almacén de datos (Storage I/O Control)
- Pertenencia de almacén de datos-centro de datos
- Pertenencia de host-almacén de datos

Distributed Power Management

Si se coloca un host en modo de espera después de realizar una copia de seguridad, es posible que vCenter Server obligue al host a salir del modo de espera cuando se restaure la copia de seguridad.

Conmutador virtual distribuido

Si utiliza un conmutador virtual distribuido, se recomienda exportar por separado la configuración de conmutador virtual distribuido antes de restaurar una copia de seguridad. La configuración se puede importar después de la restauración. Si no tiene en cuenta esta consideración, se podrían perder los cambios que se realicen en un conmutador virtual distribuido después de la copia de seguridad. Para conocer los pasos detallados, consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/2034602.

Bibliotecas de contenido

Si se eliminan bibliotecas o elementos después de realizar una copia de seguridad, no se podrá acceder a esas bibliotecas o elementos después de la restauración. Solo se podrán eliminar esas bibliotecas o elementos. Un mensaje de advertencia indicará que no se encontraron algunos archivos o carpetas en la copia de seguridad de almacenamiento.

Si se crean elementos o archivos de elementos nuevos después de realizar la copia de seguridad, no existirán registros de esos elementos en el servicio de biblioteca de contenido después de la operación de restauración. Una advertencia indicará que se encontraron archivos o carpetas adicionales en la copia de seguridad de almacenamiento.

Si se crean bibliotecas nuevas después de realizar la copia de seguridad, no existirán registros de esas bibliotecas en el servicio de biblioteca de contenido después de la restauración. El contenido de las bibliotecas existirá en la copia de seguridad de almacenamiento, pero no se mostrará ninguna advertencia. El usuario deberá limpiar manualmente las bibliotecas nuevas.

Operaciones de ciclo de vida de máquinas virtuales

- Restauración de vCenter Server a partir de una copia de seguridad realizada durante operaciones de reubicación en proceso en la instancia de vCenter Server.

Después de restaurar vCenter Server, es posible que la vista de máquinas virtuales de vCenter Server quede desincronizada con la vista de máquinas virtuales de ESXi. Esto también sucede si la copia de seguridad se realizó durante operaciones en proceso en vCenter Server. Si las máquinas virtuales desaparecen después de restaurar vCenter Server, puede consultar los siguientes casos.

a La máquina virtual desaparecida se encuentra ubicada en el host ESXi de destino y registrada en el host ESXi de destino, pero está huérfana o no se encuentra en el inventario de vCenter Server. Es necesario agregar manualmente la máquina virtual al inventario de vCenter Server.

b La máquina virtual desaparecida se encuentra ubicada en el host ESXi de destino, pero no está registrada en el host ESXi de destino y no se muestra en el inventario de vCenter Server. Es necesario registrar manualmente la máquina virtual en el host ESXi y volver a agregarla al inventario de vCenter Server.

c La máquina virtual desaparecida se encuentra ubicada en el host ESXi de destino, pero no está registrada en el host ESXi de destino. En la instancia de vCenter Server, la máquina virtual desaparecida se marca como huérfana. Es necesario eliminar la máquina virtual del inventario de vCenter Server y agregarla de nuevo.

- Restauración de vCenter Server a partir de una copia de seguridad que tiene un diseño de máquina virtual de clon vinculado desactualizado.

  Si crea una máquina virtual de clonación vinculada después de la copia de seguridad y restaura vCenter Server desde la copia de seguridad anterior, después de la restauración, vCenter Server no conoce la existencia de la nueva máquina virtual de clonación vinculada hasta que vCenter Server detecta la nueva máquina virtual de clonación vinculada. Si se eliminan todas las máquinas virtuales existentes antes de detectar la nueva máquina virtual de clon vinculado, la eliminación de las máquinas virtuales existentes daña al nuevo clon vinculado debido a la desaparición de los discos. Para evitar esto, se debe esperar hasta que vCenter Server detecte todas las máquinas virtuales de clon vinculado antes de eliminar máquinas virtuales.

- Restaurar vCenter Server a partir de una copia de seguridad que se realizó durante el registro de la máquina virtual.

  Si registra una máquina virtual durante la copia de seguridad y restaura vCenter Server a partir de la copia de seguridad antigua, tras la restauración, la máquina virtual se marcará como huérfana en la instancia de vCenter Server. Es necesario agregar manualmente la máquina virtual al inventario de vCenter Server.

vSphere High Availability

La restauración de vCenter Server a partir de una copia de seguridad puede producir una reversión a una versión anterior de estado del clúster de vSphere HA (Lista de hosts, Configuración de clúster, Estado de protección de la máquina virtual) mientras los hosts del clúster tengan la versión más reciente de estado del clúster. Debe asegurarse de que el estado del clúster de vSphere HA no sufra modificaciones durante las operaciones de restauración y copia de seguridad. De lo contrario, se pueden producir los siguientes problemas.

- Si se agregan o eliminan hosts en el clúster de vSphere HA después de una copia de seguridad y antes de la restauración de vCenter Server, es posible que las máquinas virtuales entren en conmutación por error con hosts que vCenter Server no administra, pero forman parte del clúster de HA.
- El estado de protección de las máquinas virtuales nuevas no se actualiza en agentes de vSphere HA en hosts que forman parte de un clúster de vSphere HA. Como resultado, las máquinas virtuales quedan sin protección o desprotegidas.
- El estado de configuración de los clústeres nuevos no se actualiza en agentes de vSphere HA en hosts que forman parte de un clúster de vSphere HA.

vCenter High Availability

La restauración de vCenter Server requiere que se vuelva a configurar vCenter HA.

Administración de almacenamiento basada en directivas

La restauración de vCenter Server a partir de una copia de seguridad puede producir las siguientes inconsistencias en directivas de almacenamiento, proveedores de almacenamiento y máquinas virtuales.

- Los proveedores de almacenamiento registrados después de la copia de seguridad se pierden.
- Los proveedores de almacenamiento no registrados después de la copia de seguridad reaparecen, y pueden mostrar otro estado del proveedor.
- Los cambios, como crear, eliminar o actualizar, realizados en las directivas de almacenamiento después de la copia de seguridad se pierden.
- Los cambios, como crear, eliminar o actualizar, realizados en los componentes de las directivas de almacenamiento después de la copia de seguridad se pierden.
- Los cambios en la configuración de directivas predeterminada para los almacenes de datos realizados después de la copia de seguridad se pierden.
- Pueden producirse cambios en la asociación de directivas de almacenamiento de la máquina virtual y sus discos, y en su cumplimiento de las directivas.

Red de área de almacenamiento virtual

La restauración de vCenter Server a partir de una copia de seguridad puede provocar inconsistencias en vSAN. Para obtener información sobre la forma de comprobar el estado de vSAN, consulte *Administrar VMware vSAN*.

Aplicación de revisiones

La restauración de vCenter Server a partir de una copia de seguridad puede producir la desaparición de revisiones de seguridad. Debe volver a aplicarlas una vez se complete la restauración. Para obtener información sobre la aplicación de revisiones en vCenter Server Appliance, consulte *Actualizar vSphere*.

Realizar una copia de seguridad de vCenter Server Appliance mediante la interfaz de administración de vCenter Server Appliance

Se puede usar la interfaz de administración de vCenter Server Appliance para realizar una copia de seguridad de la instancia de vCenter Server. Puede seleccionar si el archivo de copia de seguridad incluirá datos históricos, como estadísticas, eventos y tareas.

Nota La operación de copia de seguridad de un clúster de vCenter High Availability solo incluye al nodo activo.

Requisitos previos

- Debe tener un servidor FTP, FTPS, HTTP, HTTPS o SCP en funcionamiento, con suficiente espacio en disco para poder almacenar la copia de seguridad.
- Reserve una carpeta en el servidor para cada copia de seguridad basada en archivos.

Procedimiento

1. En un explorador web, vaya a la interfaz de administración de vCenter Server Appliance, https://*appliance-IP-address-or-FQDN*:5480.
2. Inicie sesión como raíz.
3. En la interfaz de administración de vCenter Server Appliance, haga clic en **Resumen**.
4. Haga clic en **Copia de seguridad**.

   Se abrirá el asistente **Copia de seguridad de dispositivo**.

5 Introduzca los detalles de la ubicación y del protocolo de copia de seguridad.

Opción	Descripción
Protocolo de copia de seguridad	Seleccione el protocolo que usará para conectarse al servidor de copia de seguridad. Puede elegir FTP, FTPS, HTTP, HTTPS o SCP. Para FTP, FTPS, HTTP o HTTPS, la ruta de acceso depende del directorio de inicio configurado para el servicio. Para SCP, la ruta de acceso es exclusiva del directorio raíz de los sistemas remotos.
Ubicación de la copia de seguridad	Introduzca la dirección del servidor y la carpeta de copia de seguridad donde almacenará los archivos de copia de seguridad.
Puerto	Introduzca el puerto predeterminado o personalizado del servidor de copia de seguridad.
Nombre de usuario	Escriba el nombre de usuario de un usuario con privilegios de **escritura** sobre el servidor de copia de seguridad.
Contraseña	Escriba la contraseña del usuario con privilegios de **escritura** sobre el servidor de copia de seguridad.

6 (opcional) Seleccione **Cifrar datos de copia de seguridad** para cifrar el archivo de copia de seguridad e introduzca una contraseña de cifrado.

   Si elige cifrar los datos de copia de seguridad, deberá usar la contraseña de cifrado para el proceso de restauración.

7 Haga clic en **Siguiente**.

8 En la página Seleccione las partes por incluir en la copia de seguridad, revise los datos incluidos en la copia de seguridad de forma predeterminada.

9 (opcional) Seleccione **Estadísticas, eventos y tareas** para hacer una copia de seguridad adicional de los datos históricos de la base de datos.

10 (opcional) En el cuadro de texto **Descripción**, escriba una descripción de la copia de seguridad y haga clic en **Siguiente**.

11 En la página Listo para finalizar, revise la información de resumen de la copia de seguridad y haga clic en **Finalizar**.

   Se abrirá la ventana **Progreso de la copia de seguridad**, donde se indica el progreso de la operación de copia de seguridad.

12 Una vez finalizado este proceso, haga clic en **Aceptar** para cerrar la ventana **Progreso de la copia de seguridad**.

Resultados

Creó correctamente un archivo de copia de seguridad de vCenter Server Appliance.

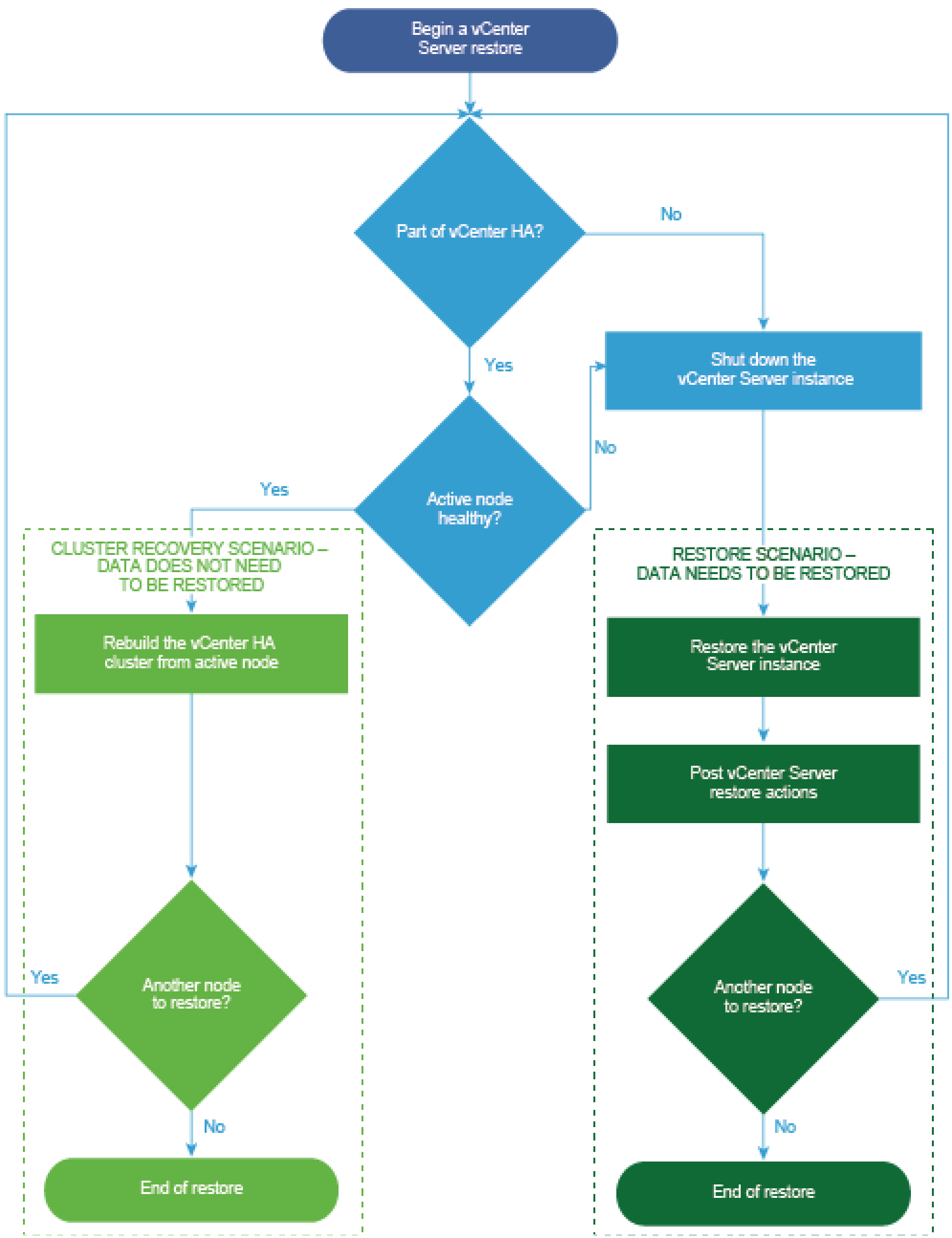
Pasos siguientes

Si se produjo un error en la copia de seguridad basada en archivos, cancele la tarea de copia de seguridad.

Restaurar una instancia de vCenter Server Appliance desde una copia de seguridad basada en archivos

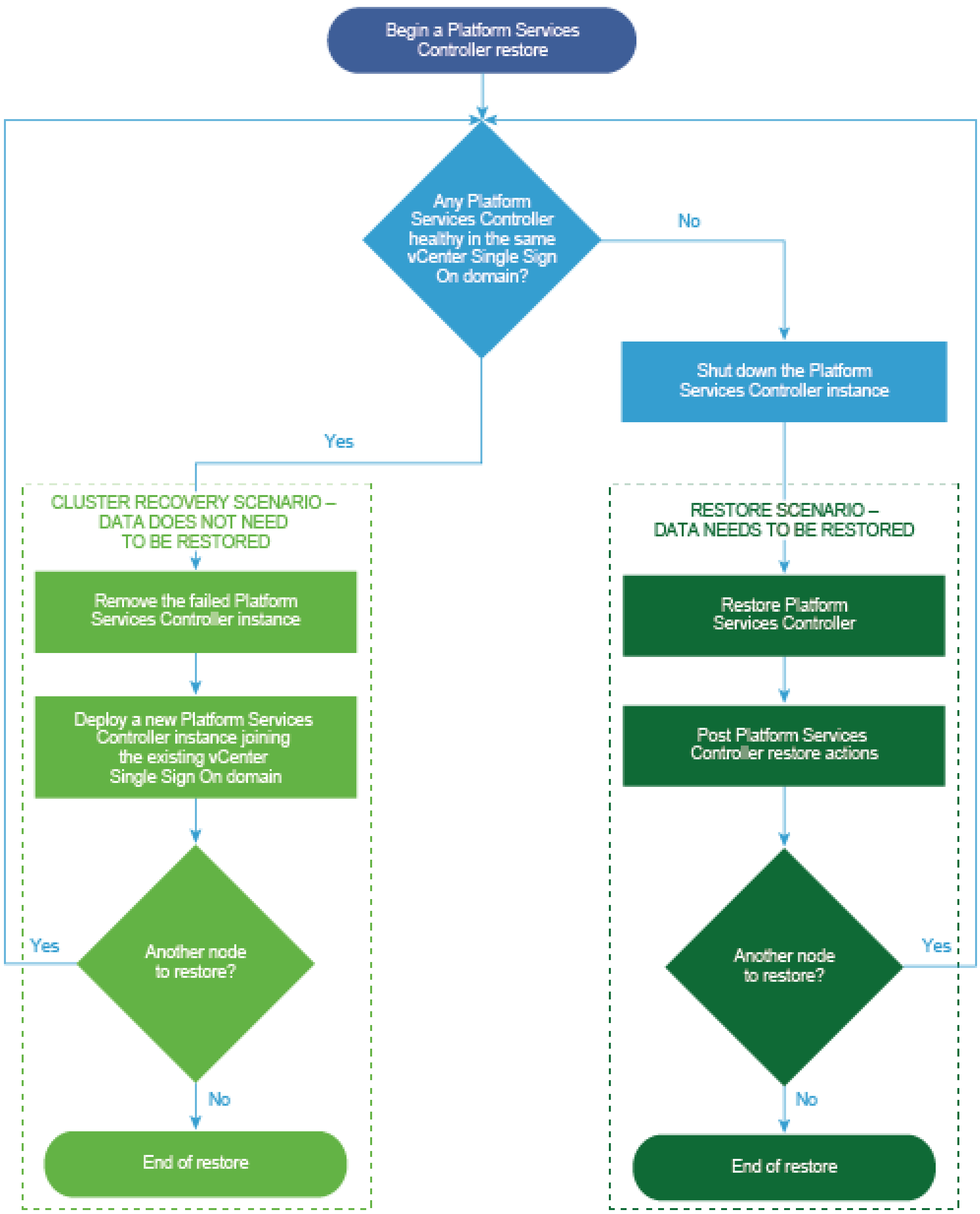
Puede usar el instalador de GUI de vCenter Server Appliance para restaurar una instancia de vCenter Server Appliance en un host ESXi o en una instancia de vCenter Server. El procedimiento de restauración tiene dos etapas. En la primera etapa, se implementa una nueva instancia de vCenter Server Appliance. En la segunda etapa, se rellena la instancia de vCenter Server Appliance recién implementada con los datos almacenados en la copia de seguridad basada en archivos.

Figura 6-1. Flujo de trabajo de restauración de vCenter Server Appliance



La restauración basada en archivos de una instancia de Platform Services Controller solo puede realizarse cuando se produce un error en la última instancia de Platform Services Controller del dominio. Si hay otras instancias de Platform Services Controller en el mismo dominio de vCenter Single Sign-On, implemente una nueva instancia de Platform Services Controller y asóciela al dominio de Single Sign-On existente.

Figura 6-2. Flujo de trabajo de restauración del dispositivo de Platform Services Controller



Requisitos previos

- Compruebe que su sistema cumpla con los requisitos mínimos de hardware y software. Consulte Requisitos de sistema para el dispositivo vCenter Server Appliance y Platform Services Controller.

- Descargar y montar el instalador de vCenter Server Appliance.
- Si la instancia de vCenter Server forma parte de un clúster de vCenter High Availability, debe apagar los nodos activo, pasivo y testigo del clúster antes de restaurar vCenter Server.

Procedimiento

1 Etapa 1: Implementar un nuevo dispositivo

  En la etapa 1 del proceso de restauración, se implementa el archivo OVA, que está incluido en el instalador de GUI de vCenter Server Appliance.

2 Etapa 2: Transferir datos al dispositivo recién implementado

  Cuando termina la implementación de OVA, se lo redirige a la etapa 2 del proceso de restauración, en el cual los datos de la ubicación de la copia de seguridad se copian en el dispositivo de vCenter Server Appliance recién implementado.

Etapa 1: Implementar un nuevo dispositivo

En la etapa 1 del proceso de restauración, se implementa el archivo OVA, que está incluido en el instalador de GUI de vCenter Server Appliance.

Como alternativa a la primera etapa de la restauración con el instalador de GUI, puede implementar el archivo OVA de la nueva instancia de vCenter Server Appliance o del nuevo dispositivo de Platform Services Controller mediante el uso de vSphere Web Client o VMware Host Client. Para implementar el archivo OVA en un host ESXio una instancia de vCenter Server 5.5 o 6.0, puede también usar vSphere Client. Después de la implementación de OVA, debe iniciar sesión en la interfaz de administración de dispositivos del dispositivo recién implementado para seguir con la segunda etapa del proceso de restauración.

Requisitos previos

- Descargue el instalador de vCenter Server Appliance y móntelo. Consulte Descargar y montar el instalador de vCenter Server Appliance.
- Si desea restaurar vCenter Server Appliance en un host ESXi, compruebe que el host ESXi de destino no esté en modo de bloqueo o de mantenimiento.
- Si desea restaurar vCenter Server Appliance en un clúster de DRS de un inventario de vCenter Server, compruebe que el clúster contenga al menos un host ESXi que no esté en modo de bloqueo o de mantenimiento.
- Si desea asignar una dirección IP estática al dispositivo, compruebe que se hayan configurado los registros de DNS inversos y directos para la dirección IP.
- Si intenta restaurar una instancia de vCenter Server que aún está en ejecución, antes de iniciar la operación de restauración debe apagar la instancia de vCenter Server incluida en la copia de seguridad.

Procedimiento

1. En el instalador de vCenter Server Appliance, desplácese hasta el directorio `vcsa-ui-installer`, vaya al subdirectorio del sistema operativo y ejecute el instalador.
   - En un sistema operativo Windows, vaya al subdirectorio `win32` y ejecute el archivo `installer.exe`.
   - En un sistema operativo Linux, vaya al subdirectorio `lin64` y ejecute el archivo `installer`.
   - En un sistema operativo Mac OS, vaya al subdirectorio `mac` y ejecute el archivo `Installer.app`.
2. En la página de inicio, haga clic en **Restaurar**.
3. Revise la página de introducción para comprender el proceso de restauración y haga clic en **Siguiente**.
4. Lea y acepte el contrato de licencia, y haga clic en **Siguiente**.
5. En la página Introducir los detalles de la copia de seguridad, introduzca los detalles del archivo de copia de seguridad que desea restaurar y haga clic en **Siguiente**.

Opción	Descripción
Tipo de ubicación de la copia de seguridad	Seleccione el protocolo que usará para recuperar la copia de seguridad del servidor de copia de seguridad. Puede elegir HTTPS, HTTP, SCP, FTPS o FTP.
Ubicación de la copia de seguridad	Introduzca la dirección del servidor y la carpeta de copia de seguridad donde están almacenados los archivos de copia de seguridad.
Puerto	Introduzca el puerto predeterminado o personalizado del servidor de copia de seguridad.
Nombre de usuario	Escriba el nombre de usuario de un usuario con privilegios de **lectura** sobre el servidor de copia de seguridad.
Contraseña	Escriba la contraseña del usuario con privilegios de **lectura** sobre el servidor de copia de seguridad.
Contraseña de cifrado	Si el archivo de copia de seguridad está cifrado, introduzca la contraseña de cifrado.

6. Revise la información de la copia de seguridad y haga clic en **Siguiente**.

7 Conéctese al host ESXi o a la instancia de vCenter Server en la cual desea implementar la instancia de vCenter Server Appliance que usará para la operación de restauración.

Opción	Pasos
Puede conectarse al host ESXi en el que desea implementar el dispositivo que usará para la operación de restauración.	1 Escriba el FQDN o la dirección IP del host ESXi. 2 Especifique el puerto HTTPS del host ESXi. 3 Especifique el nombre de usuario y la contraseña de un usuario con privilegios de administrador en el host ESXi (por ejemplo, el usuario raíz). 4 Haga clic en **Siguiente**. 5 Asegúrese de que la advertencia de certificado muestre la huella digital SHA1 del certificado SSL que se instaló en el host ESXi de destino y haga clic en **Sí** para aceptar la huella digital del certificado.
Puede conectarse a una instancia de vCenter Server y examinar el inventario para seleccionar el host ESXi o el clúster de DRS donde desea implementar el dispositivo que usará para la operación de restauración.	1 Escriba el nombre de dominio completo o la dirección IP de la instancia de vCenter Server. 2 Especifique el puerto HTTPS de la instancia de vCenter Server. 3 Especifique el nombre de usuario y la contraseña de un usuario con privilegios administrativos de vCenter Single Sign-On en la instancia de vCenter Server (por ejemplo, el usuario administrator@*your_domain_name*). 4 Haga clic en **Siguiente**. 5 Asegúrese de que la advertencia de certificado muestre la huella digital SHA1 del certificado SSL que se instaló en la instancia de vCenter Server de destino y haga clic en **Sí** para aceptar la huella digital del certificado. 6 Seleccione el centro de datos o la carpeta de centro de datos que contienen el host ESXi o el clúster de DRS donde desea implementar el dispositivo y haga clic en **Siguiente**. **Nota** Es necesario seleccionar un centro de datos o una carpeta de centro de datos que contenga al menos un host ESXi que no se encuentre en modo de bloqueo o de mantenimiento. 7 Seleccione el host ESXi o el clúster de DRS donde desea implementar el dispositivo y haga clic en **Siguiente**.

8 Acepte la advertencia de certificado.

9 Escriba un nombre para vCenter Server Appliance, establezca la contraseña del usuario raíz y haga clic en **Siguiente**.

10 Seleccione el tamaño de implementación de la nueva instancia de vCenter Server Appliance según el tamaño del inventario de vSphere.

Opción de tamaño de implementación	Descripción
Muy pequeño	Implementa un dispositivo con 2 CPU y 10 GB de memoria. Apropiado para entornos con hasta 10 hosts o 100 máquinas virtuales.
Pequeño	Implementa un dispositivo con 4 CPU y 16 GB de memoria. Apropiado para entornos con hasta 100 hosts o 1.000 máquinas virtuales.
Mediano	Implementa un dispositivo con 8 CPU y 24 GB de memoria. Apropiado para entornos con hasta 400 hosts o 4.000 máquinas virtuales.

Opción de tamaño de implementación	Descripción
Grande	Implementa un dispositivo con 16 CPU y 32 GB de memoria. Apropiado para entornos con hasta 1.000 hosts o 10.000 máquinas virtuales.
Extra grande	Implementa un dispositivo con 24 CPU y 48 GB de memoria. Apropiado para entornos con hasta 2.000 hosts o 35.000 máquinas virtuales.

11 Seleccione el tamaño de almacenamiento de la nueva instancia de vCenter Server Appliance y haga clic en **Siguiente**.

Importante Debe tener en cuenta el tamaño de almacenamiento del dispositivo que desea restaurar.

Opción de tamaño de almacenamiento	Descripción de tamaño de implementación muy pequeño	Descripción de tamaño de implementación pequeño	Descripción de tamaño de implementación mediano	Descripción de tamaño de implementación grande	Descripción de tamaño de implementación extragrande
Predeterminado	Implementa un dispositivo con 250 GB de almacenamiento.	Implementa un dispositivo con 290 GB de almacenamiento.	Implementa un dispositivo con 425 GB de almacenamiento.	Implementa un dispositivo con 640 GB de almacenamiento.	Implementa un dispositivo con 980 GB de almacenamiento.
Grande	Implementa un dispositivo con 775 GB de almacenamiento.	Implementa un dispositivo con 820 GB de almacenamiento.	Implementa un dispositivo con 925 GB de almacenamiento.	Implementa un dispositivo con 990 GB de almacenamiento.	Implementa un dispositivo con 1.030 GB de almacenamiento.
Extragrande	Implementa un dispositivo con 1.650 GB de almacenamiento.	Implementa un dispositivo con 1.700 GB de almacenamiento.	Implementa un dispositivo con 1.805 GB de almacenamiento.	Implementa un dispositivo con 1.870 GB de almacenamiento.	Implementa un dispositivo con 1.910 GB de almacenamiento.

12 En la lista de almacenes de datos disponibles, seleccione la ubicación en la que se almacenarán todos los archivos de configuración y discos virtuales de la máquina virtual. Opcionalmente, seleccione **Habilitar el modo de disco fino** para habilitar el aprovisionamiento fino.

13 En la página Ajustar la configuración de red, revise la configuración que se carga a partir del archivo de copia de seguridad de vCenter Server Appliance.

14 (opcional) Edite la configuración de red para que coincida con el entorno de red actual donde está almacenado el dispositivo de vCenter Server Appliance.

15 En la página Listo para finalizar la etapa 1, revise la configuración de implementación para la instancia restaurada de vCenter Server Appliance y haga clic en **Finalizar** para iniciar el proceso de implementación de OVA.

16 Espere a que finalice la implementación de OVA y haga clic en **Continuar** para pasar a la etapa 2 del proceso de restauración a fin de transferir los datos al dispositivo recién implementado.

Nota Si hace clic en **Cerrar** para salir del asistente, deberá iniciar sesión en la interfaz de administración de vCenter Server Appliance para transferir los datos.

Resultados

La instancia de vCenter Server Appliance recién implementada se ejecuta en el servidor de destino, pero los datos no se copian desde la ubicación de la copia de seguridad.

Etapa 2: Transferir datos al dispositivo recién implementado

Cuando termina la implementación de OVA, se lo redirige a la etapa 2 del proceso de restauración, en el cual los datos de la ubicación de la copia de seguridad se copian en el dispositivo de vCenter Server Appliance recién implementado.

Procedimiento

1 Revise la introducción a la etapa 2 del proceso de restauración y haga clic en **Siguiente**.

2 Revise los detalles de la copia de seguridad y haga clic en **Siguiente**.

3 En la página Listo para finalizar, revise los detalles, haga clic en **Finalizar** y, luego, en **Aceptar** para completar la etapa 2 del proceso de restauración.

   Este proceso reinicia el servicio de administración de vCenter Server Appliance. No se puede acceder a la API de administración de vCenter Server Appliance durante el reinicio.

   Importante Si se produce un error en la operación de restauración de un vCenter Server Appliance o una máquina virtual del dispositivo de Platform Services Controller, debe apagar la máquina virtual que se ha restaurado parcialmente y eliminarla. A continuación, podrá intentar restaurar la máquina virtual de nuevo.

4 (opcional) Después de que se complete el proceso de restauración, haga clic en **https://*vcenter_server_appliance_fqdn*/vsphere-client** para ir a vSphere Web Client e iniciar sesión en la instancia de vCenter Server en vCenter Server Appliance, o bien haga clic en **https://*vcenter_server_appliance_fqdn*:443** para ir a la página de introducción de vCenter Server Appliance.

5 Haga clic en **Cerrar** para cerrar el asistente.

   Se abrirá la página de introducción de vCenter Server Appliance.

6 Para completar el proceso de restauración, realice una operación de recuperación posterior.

Tipo de nodo restaurado	Acción
vCenter Server Appliance con una instancia de Platform Services Controller externa	a Inicie sesión en el shell de Bash de vCenter Server Appliance. b Ejecute el script `/usr/bin/vcenter-restore`.
Dispositivo Platform Services Controller	Para todos los nodos de vCenter Server del dominio a Inicie sesión en el shell de Bash de vCenter Server Appliance. b Ejecute el script `/usr/bin/vcenter-restore`.
vCenter Server Appliance con una instancia de Platform Services Controller integrada	La recuperación posterior a la restauración no es un paso obligatorio para este tipo de nodo.

7 Si el nodo de vCenter con copia de seguridad forma parte de un clúster de vCenter High Availability, es necesario volver a configurar el clúster una vez que la operación de restauración se complete correctamente.

Para obtener información sobre cómo realizar operaciones de copia de seguridad y restauración, consulte *Disponibilidad de vSphere*.

Restaurar y crear copias de seguridad con base en imágenes de un entorno de vCenter Server

7

Puede utilizar vSphere Data Protection o un producto de otro proveedor integrado con VMware vSphere Storage APIs - Data Protection para hacer copias de seguridad y restaurar una máquina virtual que contenga instancias de vCenter Server, vCenter Server Appliance o Platform Services Controller.

vSphere Data Protection es una solución de copia de seguridad y recuperación suministrada por EMC. vSphere Data Protection se integra completamente con vCenter Server y permite administrar los trabajos de copia de seguridad y, al mismo tiempo, almacenar las copias de seguridad en ubicaciones de almacenamiento de destino desduplicadas. Después de implementar y configurar vSphere Data Protection, puede acceder a vSphere Data Protection mediante la interfaz de vSphere Web Client para seleccionar, programar, configurar y administrar copias de seguridad y recuperaciones de máquinas virtuales. Durante la copia de seguridad, vSphere Data Protection crea una instantánea en modo inactivo para la máquina virtual. La desduplicación se ejecuta de manera automática con cada copia de seguridad.

Puede utilizar vSphere Data Protection para realizar una copia de seguridad completa basada en imágenes de una máquina virtual que contiene una instancia de vCenter Server, vCenter Server Appliance o Platform Services Controller. La máquina virtual debe usar un FQDN con la resolución de DNS correcta, o el nombre de host debe estar configurado para ser una dirección IP. Si el nombre de host está configurado como una dirección IP, no es posible cambiarla.

Las siguientes copias de seguridad y recuperaciones no son compatibles con vSphere Data Protection:

- Copias de seguridad incrementales
- Copias de seguridad diferenciales
- Copias de seguridad de discos individuales
- Máquinas virtuales con instantáneas
- Máquinas virtuales configuradas con Fault Tolerance

Alternativamente a vSphere Data Protection, puede utilizar productos de otros proveedores integrados con VMware vSphere Storage APIs - Data Protection.

VMware vSphere Storage APIs - Data Protection es un marco de protección de datos que habilita las copias de seguridad de los productos para realizar copias de seguridad centralizadas, efectivas, fuera del host y sin utilizar la red LAN de las máquinas virtuales vSphere. Para obtener información acerca de VMware vSphere Storage APIs - Data Protection, visite el sitio web de VMware. Para obtener información acerca de la integración de productos de copia de seguridad con VMware vSphere Storage APIs - Data Protection, póngase en contacto con su proveedor de copias de seguridad.

Este capítulo incluye los siguientes temas:

Consideraciones y limitaciones para copias de seguridad y restauraciones basadas en imágenes

Al restaurar un entorno de vCenter Server, tenga en cuenta estas consideraciones y limitaciones.

Nota La restauración de una instancia de vCenter Server o Platform Services Controller con configuración de red DHCP provoca una modificación en su dirección IP. La dirección IP modificada impide que algunos servicios de vCenter Server se inicien correctamente. Para iniciar correctamente todos los servicios de vCenter Server, después de la restauración, se debe volver a configurar la dirección IP de la instancia de vCenter Server o Platform Services Controller restaurada con la dirección IP que tenía esta instancia cuando se realizó la copia de seguridad.

Configuración

Después de una restauración, las siguientes configuraciones se revierten al estado que tenían cuando se realizó la copia de seguridad.

- Configuración de recursos de máquinas virtuales
- Jerarquía y configuración del grupo de recursos
- Pertenencia de clúster-host
- Reglas y configuración de DRS

Storage DRS

Si se modifica la configuración, es posible que las siguientes opciones cambien después de una restauración.

- Configuración del clúster de almacén de datos
- Pertenencia del clúster de almacén de datos

- Opciones de administración de recursos de E/S del almacén de datos (Storage I/O Control)
- Pertenencia de almacén de datos-centro de datos
- Pertenencia de host-almacén de datos

Distributed Power Management

Si se coloca un host en modo de espera después de realizar una copia de seguridad, es posible que vCenter Server obligue al host a salir del modo de espera cuando se restaure la copia de seguridad.

Conmutador virtual distribuido

Si utiliza un conmutador virtual distribuido, se recomienda exportar por separado la configuración de conmutador virtual distribuido antes de restaurar una copia de seguridad. La configuración se puede importar después de la restauración. Si no tiene en cuenta esta consideración, se podrían perder los cambios que se realicen en un conmutador virtual distribuido después de la copia de seguridad. Para conocer los pasos detallados, consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/2034602.

Bibliotecas de contenido

Si se eliminan bibliotecas o elementos después de realizar una copia de seguridad, no se podrá acceder a esas bibliotecas o elementos después de la restauración. Solo se podrán eliminar esas bibliotecas o elementos. Un mensaje de advertencia indicará que no se encontraron algunos archivos o carpetas en la copia de seguridad de almacenamiento.

Si se crean elementos o archivos de elementos nuevos después de realizar la copia de seguridad, no existirán registros de esos elementos en el servicio de biblioteca de contenido después de la operación de restauración. Una advertencia indicará que se encontraron archivos o carpetas adicionales en la copia de seguridad de almacenamiento.

Si se crean bibliotecas nuevas después de realizar la copia de seguridad, no existirán registros de esas bibliotecas en el servicio de biblioteca de contenido después de la restauración. El contenido de las bibliotecas existirá en la copia de seguridad de almacenamiento, pero no se mostrará ninguna advertencia. El usuario deberá limpiar manualmente las bibliotecas nuevas.

Operaciones de ciclo de vida de máquinas virtuales

- Restauración de vCenter Server desde una copia de seguridad que se realizó mientras había operaciones de reubicación en proceso dentro de la instancia de vCenter Server.

Después de restaurar vCenter Server, la vista de vCenter Server de las máquinas virtuales puede estar desincronizada con la vista de ESXi de las máquinas virtuales. Esto también sucede si realizó la copia de seguridad mientras había operaciones en proceso en la instancia de vCenter Server. Si las máquinas virtuales desaparecen después de restaurar vCenter Server, puede consultar los siguientes casos.

a La máquina virtual desaparecida se encuentra ubicada en el host ESXi de destino y registrada en el host ESXi de destino, pero no se muestra en el inventario de vCenter Server. Es necesario agregar manualmente la máquina virtual al inventario de vCenter Server.

b La máquina virtual desaparecida se encuentra ubicada en el host ESXi de destino, pero no está registrada en el host ESXi de destino y no se muestra en el inventario de vCenter Server. Debe registrar manualmente la máquina virtual en la instancia de ESXi y agregarla nuevamente al inventario de vCenter Server.

c La máquina virtual desaparecida se encuentra ubicada en el host ESXi de destino, pero no está registrada en el host ESXi de destino. Dentro de la instancia de vCenter Server, la máquina virtual que falta está marcada como huérfana. Es necesario eliminar la máquina virtual del inventario de vCenter Server y agregarla de nuevo.

- Restauración de vCenter Server desde una copia de seguridad que posee un diseño desactualizado de máquina virtual de clonación vinculada.

  Si crea una máquina virtual de clonación vinculada después de la copia de seguridad y restaura vCenter Server desde la copia de seguridad anterior, después de la restauración, vCenter Server no conoce la existencia de la nueva máquina virtual de clonación vinculada hasta que vCenter Server detecta la nueva máquina virtual de clonación vinculada. Si se eliminan todas las máquinas virtuales existentes antes de detectar la nueva máquina virtual de clon vinculado, la eliminación de las máquinas virtuales existentes daña al nuevo clon vinculado debido a la desaparición de los discos. Para evitar esta situación, debe esperar hasta que vCenter Server detecte todas las máquinas virtuales de clonación vinculada antes de eliminar las máquinas virtuales.

vSphere High Availability

La restauración de vCenter Server desde una copia de seguridad puede provocar una reversión a una versión anterior en el estado del clúster de vSphere HA (HostList, ClusterConfiguration, estado de protección de la máquina virtual) mientras los hosts en el clúster tienen la versión más reciente del estado del clúster. Asegúrese de que el estado del clúster de vSphere HA no sufra modificaciones durante las operaciones de restauración y copia de seguridad. De lo contrario, se pueden hacer presentes los siguientes problemas.

- Si se agregan o se eliminan hosts en el clúster de vSphere HA después de un copia de seguridad y antes de la restauración de vCenter Server, las máquinas virtuales potencialmente podrían conmutar por error a hosts que no son administrados por vCenter Server, pero siguen formando parte del clúster de HA.

- Los estados de protección para las nuevas máquinas virtuales no se actualizan en los agentes de vSphere HA presentes en los hosts que forman parte del clúster de vSphere HA. Como resultado, las máquinas virtuales quedan sin protección o desprotegidas.
- El estado de configuración de los clústeres nuevos no se actualiza en agentes de vSphere HA en hosts que forman parte de un clúster de vSphere HA.

vCenter High Availability

La restauración de vCenter Server requiere que se vuelva a configurar vCenter HA.

Administración de almacenamiento basada en directivas

La restauración de vCenter Server a partir de una copia de seguridad puede producir las siguientes inconsistencias en directivas de almacenamiento, proveedores de almacenamiento y máquinas virtuales.

- Los proveedores de almacenamiento registrados después de la copia de seguridad se pierden.
- Los proveedores de almacenamiento no registrados después de la copia de seguridad reaparecen y podrían mostrar otro estado del proveedor.
- Los cambios, como crear, eliminar o actualizar, realizados en las directivas de almacenamiento después de la copia de seguridad se pierden.
- Los cambios, como crear, eliminar o actualizar, realizados en los componentes de las directivas de almacenamiento después de la copia de seguridad se pierden.
- Los cambios en la configuración de directivas predeterminada para los almacenes de datos realizados después de la copia de seguridad se pierden.
- Pueden producirse cambios en la asociación de directivas de almacenamiento de la máquina virtual y sus discos, y en su cumplimiento de las directivas.

Red de área de almacenamiento virtual

La restauración de vCenter Server desde una copia de seguridad puede provocar incoherencias en vSAN. Para obtener información sobre cómo comprobar el estado de vSAN, consulte *Administrar VMware vSAN*.

Aplicación de revisiones

La restauración de vCenter Server a partir de una copia de seguridad puede producir la desaparición de revisiones de seguridad. Debe volver a aplicarlas una vez se complete la restauración. Para obtener información sobre la aplicación de revisiones en vCenter Server Appliance, consulte *Actualizar vSphere*.

Usar vSphere Data Protection para hacer copias de seguridad de un entorno de vCenter Server

Para realizar una copia de seguridad basada en una imagen de una máquina virtual que contiene vCenter Server, vCenter Server Appliance o Platform Services Controller, primero debe implementar y configurar vSphere Data Protection y realizar tareas de copias de seguridad básicas.

La topología del entorno de vCenter Server puede variar y constar de muchas instancias de vCenter Server y Platform Services Controller. Siempre debe realizar copias de seguridad de todas las instancias de vCenter Server y Platform Services Controller en forma simultánea.

Importante Es posible hacer copias de seguridad únicamente de máquinas virtuales que contienen instancias de vCenter Server, vCenter Server Appliance y Platform Services Controller, y restaurarlas. No puede hacer copias de seguridad y restaurar máquinas físicas que ejecutan vCenter Server a través de vSphere Data Protection.

Procedimiento

1 Implementación de la plantilla de OVF de vSphere Data Protection

   Implemente vSphere Data Protection para realizar una copia de seguridad y restaurar las máquinas virtuales que contienen vCenter Server, vCenter Server Appliance o Platform Services Controller.

2 Configuración de vSphere Data Protection

   Durante la configuración inicial de vSphere Data Protection, puede ajustar la configuración de red y la información de zona horaria para vSphere Data Protection Appliance. Puede utilizar el asistente **Configuración de vSphere Data Protection** para registrar vSphere Data Protection Appliance con vCenter Server.

3 Crear un trabajo de copia de seguridad en vSphere Data Protection

   Es posible crear trabajos de copia de seguridad para asociar la copia de seguridad de un conjunto de una o más máquinas virtuales que contienen instancias de vCenter Server, vCenter Server Appliance y Platform Services Controller con una programación de copias de seguridad y directivas de retención específicas.

4 (Opcional) Iniciar un trabajo de copia de seguridad de forma manual

   Una operación de copia de seguridad se inicia automáticamente de acuerdo con la programación de fecha, hora y frecuencia configuradas en el trabajo de copia de seguridad. Si desea ejecutar un trabajo de copia de seguridad existente de inmediato, puede iniciar este proceso de forma manual.

Implementación de la plantilla de OVF de vSphere Data Protection

Implemente vSphere Data Protection para realizar una copia de seguridad y restaurar las máquinas virtuales que contienen vCenter Server, vCenter Server Appliance o Platform Services Controller.

Nota En este procedimiento, se utiliza vSphere Data Protection 6.1.3 para describir los pasos. Si utiliza una versión diferente de vSphere Data Protection, los pasos pueden variar.

Requisitos previos

- Compruebe que la versión de ESXi sea 5.1 o posterior.
- Si hay un firewall habilitado en el entorno, compruebe que el puerto 902 esté abierto para la comunicación entre vSphere Data Protection Appliance y el host ESXi. Consulte la documentación de *vSphere Data Protection*.
- Utilice vSphere Web Client para iniciar sesión como administrador en la instancia de vCenter Server que administra su entorno.
- Si la versión de vCenter Server es anterior a 6.5, compruebe que el complemento de integración de clientes de VMware esté instalado en el explorador. Para obtener más información, consulte la documentación de vSphere correspondiente a la versión de vCenter Server.

Procedimiento

1. Seleccione **vCenter > Centros de datos**.
2. En la pestaña **Objetos**, haga clic en **Acciones** y seleccione **Implementar plantilla de OVF**.
3. Desplácese hasta la ubicación del archivo `.ova` de vSphere Data Protection Appliance y haga clic en **Abrir**.
4. Compruebe los detalles de la plantilla de OVF y haga clic en **Siguiente**.
5. Revise los detalles de la plantilla, haga clic en **Siguiente** y siga los avisos del asistente para aceptar el contrato de licencia.
6. En la página Seleccionar nombre y carpeta, introduzca un FQDN para vSphere Data Protection Appliance, seleccione la carpeta o el centro de datos en los que desea implementar vSphere Data Protection Appliance y haga clic en **Siguiente**.

   La configuración de vSphere Data Protection usa el nombre que se introduce para buscar vSphere Data Protection Appliance en el inventario de vCenter Server. No cambie el nombre de vSphere Data Protection Appliance después de la instalación.
7. Seleccione el host en el que desea implementar vSphere Data Protection Appliance y haga clic en **Siguiente**.
8. Seleccione el formato de disco virtual y la ubicación de almacenamiento de vSphere Data Protection Appliance y haga clic en **Siguiente**.

9 Seleccione la red de destino de vSphere Data Protection Appliance y haga clic en **Siguiente**.

10 Especifique la configuración de red, como la puerta de enlace predeterminada, el DNS, la dirección IP de la red y la máscara de red, y haga clic en **Siguiente**.

Confirme que las direcciones IP sean correctas y que coincidan con el valor introducido para el servidor DNS. Si introduce direcciones IP incorrectas, deberá volver a implementar vSphere Data Protection Appliance.

Nota vSphere Data Protection Appliance no es compatible con DHCP. Se requiere una dirección IP estática.

11 En la página Listo para finalizar, confirme que todas las opciones de implementación sean correctas, seleccione **Encender después de la implementación** y haga clic en **Finalizar**.

Resultados

Se inicia el proceso de implementación de vSphere Data Protection Appliance y vSphere Data Protection Appliance arranca en modo de instalación.

Configuración de vSphere Data Protection

Durante la configuración inicial de vSphere Data Protection, puede ajustar la configuración de red y la información de zona horaria para vSphere Data Protection Appliance. Puede utilizar el asistente **Configuración de vSphere Data Protection** para registrar vSphere Data Protection Appliance con vCenter Server.

Nota En este procedimiento, se utiliza vSphere Data Protection 6.1.3 para describir los pasos. Si utiliza una versión diferente de vSphere Data Protection, los pasos pueden variar.

Requisitos previos

- Lea la *Guía de administración de vSphere Data Protection* para acceder a la lista completa de pasos para configurar vSphere Data Protection.
- Compruebe que exista espacio suficiente en el disco en el almacén de datos. Cuando se ejecuta una prueba de análisis de rendimiento opcional durante la configuración inicial de la aplicación, se requieren 41 GB para cada disco en cada almacén de datos. Si el espacio disponible es insuficiente, la prueba informa un valor de 0 para todas las pruebas de lectura, escritura y búsqueda, y muestra un estado final de espacio insuficiente.
- Utilice vSphere Web Client para iniciar sesión como administrador en la instancia de vCenter Server que administra su entorno.

Procedimiento

1 En vSphere Web Client, seleccione **Listas de inventario de vCenter > Máquinas virtuales**.

2 Haga clic con el botón derecho en vSphere Data Protection Appliance y seleccione **Abrir consola**.

Después de que se carguen los archivos de instalación, se mostrará la pantalla de bienvenida para el menú de vSphere Data Protection.

3 En un explorador web, diríjase a la dirección URL de vSphere Data Protection Configuration Utility.

https://*ip_address_VDP_Appliance*:8543/vdp-configure/

4 Inicie sesión como raíz.

La contraseña predeterminada es changeme.

Se abrirá el asistente **Configuración de vSphere Data Protection**.

5 En la página Configuración de red del asistente, introduzca o confirme la información de red y servidor para vSphere Data Protection Appliance y haga clic en **Siguiente**.

Asegúrese de que los valores se completen de forma correcta. De lo contrario, se producirá un error en la configuración inicial.

6 Seleccione la zona horaria apropiada para vSphere Data Protection Appliance y haga clic en **Siguiente**.

7 En la página Credenciales de VDP, seleccione una nueva contraseña raíz para la aplicación virtual y haga clic en **Siguiente**.

8 En la página Registro de vCenter, registre la aplicación con vCenter Server:

a En el cuadro de texto **Nombre de usuario de vCenter**, introduzca un nombre de usuario administrador de vCenter Server. Por ejemplo, **`administrator@vsphere.local`**.

Si el usuario pertenece a una cuenta de dominio, introduzca el nombre de usuario con el formato *DOMAIN\\UserName*.

Importante Si introduce el nombre de usuario de administrador de vCenter Single Sign-On con el formato de nombre principal de usuario (UPN), las tareas relacionadas con las operaciones de vSphere Data Protection no aparecerán en el panel Tareas recientes de vSphere Web Client. Si desea utilizar el nombre de usuario de administrador de vCenter Single Sign-On, introduzca el nombre de usuario de vCenter Single Sign-On con el formato UPN.

---

b En el cuadro de texto **Contraseña de vCenter**, introduzca la contraseña de vCenter Server.

c Introduzca una dirección IP o FQDN de vCenter.

d (Requerido) Cambie el puerto HTTP predeterminado de vCenter Server.

Introduzca un valor personalizado para el puerto HTTP si debe conectarse a vCenter Server a través del puerto HTTP, en lugar del puerto HTTPS, que se utiliza para todas las otras comunicaciones.

e Introduzca un puerto HTTPS de vCenter (el puerto predeterminado es 443).

f Seleccione la casilla **Utilizar vCenter para la autenticación SSO**.

g (opcional) Haga clic en **Probar conexión**.

Aparecerá un mensaje de conexión exitosa. Si este mensaje no aparece, resuelva los problemas de su configuración y repita este paso hasta que aparezca un mensaje exitoso.

9 Haga clic en **Siguiente** y responda los mensajes del asistente para completar la configuración.

Crear un trabajo de copia de seguridad en vSphere Data Protection

Es posible crear trabajos de copia de seguridad para asociar la copia de seguridad de un conjunto de una o más máquinas virtuales que contienen instancias de vCenter Server, vCenter Server Appliance y Platform Services Controller con una programación de copias de seguridad y directivas de retención específicas.

Nota En este procedimiento, se utiliza vSphere Data Protection 6.1.3 para describir los pasos. Si utiliza una versión diferente de vSphere Data Protection, los pasos pueden variar.

Requisitos previos

Utilice vSphere Web Client para iniciar sesión en la instancia de vCenter Server que administra el entorno. Inicie sesión como el usuario con privilegios de administrador que se utilizó durante la configuración de vSphere Data Protection.

Procedimiento

1 En la página de inicio de vSphere Web Client, haga clic en **vSphere Data Protection**.

2 En el menú **Acciones del trabajo de copia de seguridad**, seleccione **Nuevo** para ejecutar el asistente **Crear nuevo trabajo de copia de seguridad**.

3 En la página Tipo de trabajo, seleccione **Imágenes de invitado** y haga clic en **Siguiente**.

4 En la página Tipo de datos, seleccione **Imagen completa** y haga clic en **Siguiente**.

Puede ver todos los objetos y máquinas virtuales del inventario de vCenter Server.

5 En la página Destinos de copia de seguridad, seleccione la máquina virtual que contiene la instancia de vCenter Server o Platform Services Controller de la que desea crear una copia de seguridad y haga clic en **Siguiente**.

6 En la página Programación, seleccione la programación para el trabajo de copia de seguridad y haga clic en **Siguiente**.

7 En la página Directiva de retención, seleccione un período de retención y haga clic en **Siguiente**.

Nota Cuando introduzca un período de mantenimiento nuevo que siga a la caducidad de una copia de seguridad, vSphere Data Protection Appliance elimina su referencia a los datos de la copia de seguridad y no podrá restaurar la copia de seguridad caducada. vSphere Data Protection Appliance determina si cualquier otro punto de restauración utiliza los datos de la copia de seguridad y, si el sistema determina que no se han utilizado, los datos se eliminan y la capacidad del disco estará disponible.

8 En la página Nombre, introduzca un nombre para el trabajo de copia de seguridad y haga clic en **Siguiente**.

9 En la página Listo para completar, examine la información de resumen del trabajo de copia de seguridad y haga clic en **Finalizar**.

   El trabajo de copia de seguridad recientemente creado aparecerá incluido en una lista en la pestaña **Copia de seguridad**. El trabajo de copia de seguridad se iniciará automáticamente según la programación configurada.

(Opcional) Iniciar un trabajo de copia de seguridad de forma manual

Una operación de copia de seguridad se inicia automáticamente de acuerdo con la programación de fecha, hora y frecuencia configuradas en el trabajo de copia de seguridad. Si desea ejecutar un trabajo de copia de seguridad existente de inmediato, puede iniciar este proceso de forma manual.

Nota En este procedimiento, se utiliza vSphere Data Protection 6.1.3 para describir los pasos. Si utiliza una versión diferente de vSphere Data Protection, los pasos pueden variar.

Requisitos previos

Utilice vSphere Web Client para iniciar sesión en la instancia de vCenter Server que administra el entorno. Inicie sesión como el usuario con privilegios de administrador que se utilizó durante la configuración de vSphere Data Protection.

Procedimiento

1 En la página de inicio de vSphere Web Client, haga clic en **vSphere Data Protection**.

2 En la pestaña **Copia de seguridad**, seleccione el trabajo de copia de seguridad que desea ejecutar.

3 Haga clic en **Realizar copia de seguridad ahora** y seleccione **Realizar copia de seguridad de todas las fuentes**.

   Un cuadro de diálogo confirma que la operación de copia de seguridad se inició correctamente.

Usar vSphere Data Protection para restaurar un entorno de vCenter Server

Puede utilizar vSphere Data Protection o un producto de otro proveedor integrado con VMware vSphere Storage APIs - Data Protection para restaurar una máquina virtual que contiene una instancia de vCenter Server, vCenter Server Appliance o Platform Services Controller.

Puede utilizar vSphere Data Protection para realizar una restauración basada en imágenes de una máquina virtual que contiene una instancia de vCenter Server, vCenter Server Appliance o Platform Services Controller. La máquina virtual debe usar un FQDN con la resolución de DNS correcta, o el nombre de host del equipo debe estar configurado para ser una dirección IP. Si el nombre de host está configurado como una dirección IP, no es posible cambiarla.

Para restaurar una máquina virtual a la ubicación original, sobrescriba la máquina virtual con copia de seguridad o cree una nueva que contenga la instancia restaurada de vCenter Server, vCenter Server Appliance o Platform Services Controller en el mismo host ESXi. También puede restaurar la máquina virtual en un nuevo host ESXi.

Puede restaurar una máquina virtual que contiene una instancia de vCenter Server o Platform Services Controller directamente en el host ESXi que ejecuta vSphere Data Protection Appliance cuando el servicio de vCenter Server deja de estar disponible o cuando no se puede acceder a la interfaz de usuario de vSphere Data Protection mediante vSphere Web Client.

Importante No se admite la restauración de máquinas virtuales que tienen snapshots o que están configuradas con Fault Tolerance.

Figura 7-1. Flujo de trabajo de restauración de vCenter Server

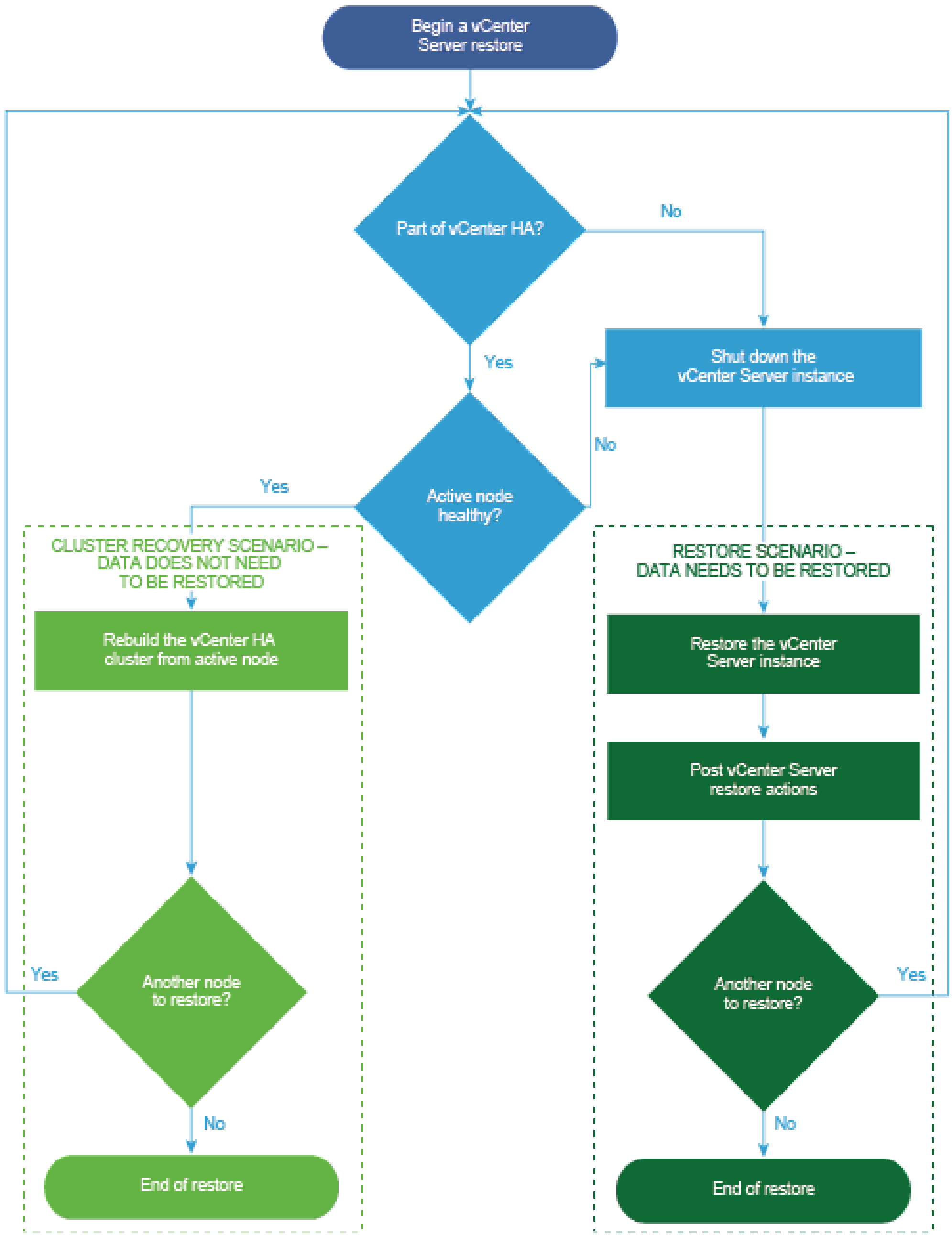
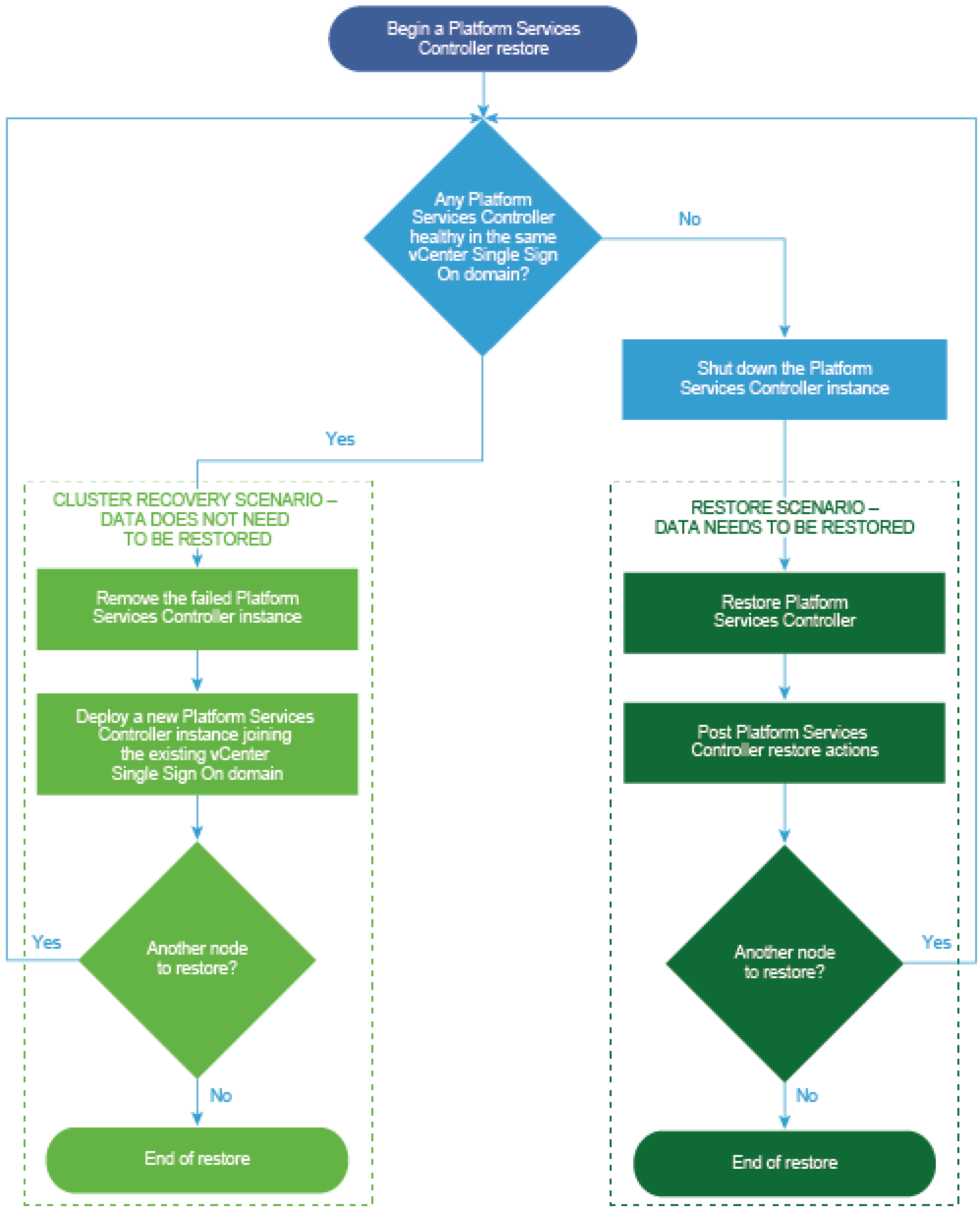


Figura 7-2. Flujo de trabajo de restauración de Platform Services Controller



Restaurar una instancia de vCenter Server con una instancia de Platform Services Controller integrada

El entorno puede estar compuesto por vCenter Server o vCenter Server Appliance con una instancia de Platform Services Controller integrada. Puede utilizar vSphere Data Protection

para restaurar un entorno de vCenter Server con una instancia de Platform Services Controller integrada.

Importante Es posible hacer copias de seguridad únicamente de máquinas virtuales que contienen instancias de vCenter Server, vCenter Server Appliance y Platform Services Controller, y restaurarlas. No puede hacer copias de seguridad y restaurar máquinas físicas que ejecutan vCenter Server a través de vSphere Data Protection.

- Restaurar la máquina virtual de vCenter Server con errores a la ubicación original

  Es posible restaurar manualmente a su ubicación original la copia de seguridad de la imagen completa de una máquina virtual que contiene vCenter Server con una instancia integrada de Platform Services Controller mediante el asistente **Restaurar copia de seguridad**.

- Restaurar la máquina virtual de vCenter Server con errores en una nueva ubicación

  Es posible restaurar manualmente la copia de seguridad de la imagen completa de una máquina virtual que contiene vCenter Server con una instancia integrada de Platform Services Controller mediante el asistente **Restaurar copia de seguridad**.

- Restaurar una máquina virtual de vCenter Server con errores mediante la operación de restauración de emergencia directa a host

  La restauración de emergencia directa a host permite restaurar la máquina virtual que contiene vCenter Server con una instancia integrada de Platform Services Controller cuando vCenter Server deja de estar disponible o cuando el usuario no puede acceder a la interfaz de usuario de vSphere Data Protection mediante vSphere Web Client.

Pasos siguientes

Encienda la máquina virtual restaurada donde se encuentra la instancia de vCenter Server restaurada.

Restaurar la máquina virtual de vCenter Server con errores a la ubicación original

Es posible restaurar manualmente a su ubicación original la copia de seguridad de la imagen completa de una máquina virtual que contiene vCenter Server con una instancia integrada de Platform Services Controller mediante el asistente **Restaurar copia de seguridad**.

Nota En este procedimiento, se utiliza vSphere Data Protection 6.1.3 para describir los pasos. Si utiliza una versión diferente de vSphere Data Protection, los pasos pueden variar.

Requisitos previos

- Implemente y configure vSphere Data Protection Appliance.
- Haga una copia de seguridad de una máquina virtual con vCenter Server en ejecución. Consulte Usar vSphere Data Protection para hacer copias de seguridad de un entorno de vCenter Server.

- Utilice vSphere Web Client para iniciar sesión en la instancia de vCenter Server que administra el entorno. Inicie sesión como el usuario con privilegios de administrador que se utilizó durante la configuración de vSphere Data Protection.
- Compruebe que la máquina virtual que desea restaurar esté apagada.

Procedimiento

1 En la página de inicio de vSphere Web Client, haga clic en **vSphere Data Protection**.

2 Haga clic en la pestaña **Restaurar**.

3 (opcional) Filtre las copias de seguridad para acotar la búsqueda.

4 Seleccione una máquina virtual de las que se enumeran en la columna Nombre y, a continuación, elija uno o más elementos de copia de seguridad que desee restaurar.

   Al seleccionar una máquina virtual, puede ver la lista de las copias de seguridad realizadas para esa máquina.

5 Haga clic en **Restaurar** para iniciar el asistente **Restaurar copia de seguridad**.

6 En la página Seleccionar copia de seguridad, compruebe que la lista de copias de seguridad sea correcta, quite las copias de seguridad que desee excluir de la operación de restauración y haga clic en **Siguiente**.

7 En la página Establecer opciones de restauración, deje seleccionada la casilla **Restaurar a la ubicación original**.

   Importante Si el disco virtual de la máquina virtual original se extrajo o se eliminó, no podrá restaurar la máquina virtual a su ubicación original. El disco de la máquina virtual (VMDK) deberá restaurarse a una ubicación nueva.

8 (opcional) En **Opciones avanzadas**, seleccione un almacén de datos nuevo para encender la máquina virtual después de que se restaure y volver a conectar la NIC.

9 Haga clic en **Siguiente**.

10 En la página Listo para completar, examine el resumen de sus solicitudes de restauración y haga clic en **Finalizar** para iniciar la operación de restauración.

   Nota Si decide volver a conectar la NIC durante el proceso de restauración, compruebe que la configuración de red de la máquina virtual recién creada sea correcta. Es posible que la NIC de la máquina virtual nueva utilice la misma dirección IP que la máquina virtual original y que eso genere conflictos.

Resultados

Un cuadro de diálogo de información confirma que la operación de restauración se inició correctamente. Puede supervisar el progreso de la restauración en el panel Tareas recientes.

Restaurar la máquina virtual de vCenter Server con errores en una nueva ubicación

Es posible restaurar manualmente la copia de seguridad de la imagen completa de una máquina virtual que contiene vCenter Server con una instancia integrada de Platform Services Controller mediante el asistente **Restaurar copia de seguridad**.

Nota En este procedimiento, se utiliza vSphere Data Protection 6.1.3 para describir los pasos. Si utiliza una versión diferente de vSphere Data Protection, los pasos pueden variar.

Requisitos previos

- Implemente y configure vSphere Data Protection Appliance.
- Haga una copia de seguridad de una máquina virtual con vCenter Server en ejecución. Consulte Usar vSphere Data Protection para hacer copias de seguridad de un entorno de vCenter Server.
- Utilice vSphere Web Client para iniciar sesión en la instancia de vCenter Server que administra el entorno. Inicie sesión como el usuario con privilegios de administrador que se utilizó durante la configuración de vSphere Data Protection.
- Compruebe que la máquina virtual que desea restaurar esté apagada.

Procedimiento

1. En la página de inicio de vSphere Web Client, haga clic en **vSphere Data Protection**.
2. Haga clic en la pestaña **Restaurar**.
3. (opcional) Filtre las copias de seguridad para acotar la búsqueda.
4. Seleccione una máquina virtual de las que se enumeran en la columna Nombre y, a continuación, elija uno o más elementos de copia de seguridad que desee restaurar.

   Al seleccionar una máquina virtual, puede ver la lista de las copias de seguridad realizadas para esa máquina.
5. Haga clic en **Restaurar** para iniciar el asistente **Restaurar copia de seguridad**.
6. En la página Seleccionar copia de seguridad, compruebe que la lista de copias de seguridad sea correcta, quite las copias de seguridad que desee excluir de la operación de restauración y haga clic en **Siguiente**.
7. En la página Establecer opciones de restauración, deseleccione la casilla **Restaurar a la ubicación original** para establecer las opciones de restauración de cada copia de seguridad que esté restaurando a una ubicación nueva.
8. Escriba el nombre de la máquina virtual nueva y haga clic en **Seleccionar** para elegir un nuevo host para la máquina virtual.
9. Seleccione el almacén de datos en el que desea restaurar la máquina virtual y haga clic en **Siguiente**.

10 (opcional) En **Opciones avanzadas**, seleccione un almacén de datos nuevo para encender la máquina virtual después de que se restaure y volver a conectar la NIC.

11 Haga clic en **Siguiente**.

12 En la página Listo para completar, examine el resumen de sus solicitudes de restauración y haga clic en **Finalizar** para iniciar la operación de restauración.

Nota Si decide volver a conectar la NIC durante el proceso de restauración, compruebe que la configuración de red de la máquina virtual recién creada sea correcta. Es posible que la NIC de la máquina virtual nueva utilice la misma dirección IP que la máquina virtual original y que eso genere conflictos.

Resultados

Un cuadro de diálogo de información confirma que la operación de restauración se inició correctamente. Puede supervisar el progreso de la restauración en el panel Tareas recientes.

Restaurar una máquina virtual de vCenter Server con errores mediante la operación de restauración de emergencia directa a host

La restauración de emergencia directa a host permite restaurar la máquina virtual que contiene vCenter Server con una instancia integrada de Platform Services Controller cuando vCenter Server deja de estar disponible o cuando el usuario no puede acceder a la interfaz de usuario de vSphere Data Protection mediante vSphere Web Client.

vSphere Data Protection depende de vCenter Server para muchas de las operaciones esenciales de vSphere Data Protection. Cuando vCenter Server deja de estar disponible, una operación de restauración de emergencia puede restaurar una máquina virtual que contiene la instancia de vCenter Server, vCenter Server Appliance o Platform Services Controller directamente en el host ESXi que se ejecuta en vSphere Data Protection Appliance. La pestaña **Restauración de emergencia** muestra una lista de máquinas virtuales que cuentan con copias de seguridad realizadas por vSphere Data Protection Appliance. Estas máquinas virtuales que contienen instancias de vCenter Server o Platform Services Controller pueden restaurarse como nuevas máquinas virtuales en el host ESXi donde se está ejecutando vSphere Data Protection Appliance. Para conocer las prácticas recomendadas, las recomendaciones y las limitaciones de la operación de restauración de emergencia, consulte la documentación de *vSphere Data Protection*.

Nota En este procedimiento, se utiliza vSphere Data Protection 6.1.3 para describir los pasos. Si utiliza una versión diferente de vSphere Data Protection, los pasos pueden variar.

Requisitos previos

Realice una copia de seguridad de la máquina virtual de vCenter Server o de vCenter Server Appliance mediante vSphere Data Protection.

Procedimiento

1. En un explorador web, desplácese hasta http://*host-name*/ui o http://*host-IP-address*/ui.

   En este caso, *host-name* es el nombre del host ESXi y *host-IP-address* es la dirección IP del host ESXi donde reside vSphere Data Protection Appliance. Inicie sesión como administrador en VMware Host Client.

   a. Haga clic con el botón derecho en **Host** desde el inventario de VMware Host Client y seleccione **Desconectar de vCenter Server** en el menú.

   b. Haga clic en **Desconectar de vCenter Server** cuando se le pida desasociar el host de vCenter Server.

   Nota Si el host ESXi es de la versión 5.1, inicie sesión en vSphere Client en lugar de hacerlo en VMware Host Client y, en la pestaña **Resumen**, haga clic en **Desasociar host de vCenter Server**.

   ---

2. En un explorador web, desplácese hasta la utilidad de configuración de vSphere Data Protection.

   https://*ip_address_VDP_Appliance*:8543/vdp-configure/.

3. En la pestaña **Restauración de emergencia**, seleccione la máquina virtual que servirá de punto de restauración y haga clic en **Restaurar**.

4. En el cuadro de diálogo Credenciales de host, ingrese credenciales de host válidas y haga clic en **Aceptar**.

5. En el cuadro de diálogo Restaurar una copia de seguridad, especifique un nombre nuevo.

6. Seleccione un almacén de datos como destino para la copia de seguridad y haga clic en **Restaurar**.

   Precaución Se enumera el tamaño de capacidad del almacén de datos. Asegúrese de seleccionar un almacén de datos con suficiente espacio en disco para admitir la restauración. Si no hay espacio suficiente, fallará la restauración.

   La máquina virtual restaurada se mostrará en el inventario en el nivel de host de vSphere. No se admite la restauración en una ruta de acceso de inventario más específica.

Restaurar un entorno de vCenter Server con una única instancia externa de Platform Services Controller

Es posible que el entorno consista en varias instancias de vCenter Server que se registran con una sola instancia de Platform Services Controller. Puede utilizar vSphere Data Protection para restaurar una máquina virtual que contiene una instancia de Platform Services Controller. También puede utilizar vSphere Data Protection para restaurar máquinas virtuales que contienen instancias

de vCenter Server o de vCenter Server Appliance que se registran con una sola instancia de Platform Services Controller externa.

Nota Si se generan errores en las instancias de vCenter Server y Platform Services Controller al mismo tiempo, primero debe restaurar las instancias de Platform Services Controller y después las de vCenter Server.

- Restaurar la instancia de Platform Services Controller con errores

  Es posible instalar e implementar Platform Services Controller, así como registrar varias instancias de vCenter Server con la misma instancia de Platform Services Controller. Es posible utilizar vSphere Data Protection para restaurar el entorno si la instancia de Platform Services Controller externa genera errores.

- Restaurar instancias de vCenter Server con errores

  Es posible instalar e implementar Platform Services Controller, así como registrar varias instancias de vCenter Server con la misma instancia de Platform Services Controller. Puede utilizar vSphere Data Protection para restaurar todo el entorno, de modo que si alguna de las instancias de vCenter Server presenta errores, sea posible restaurar la instancia de vCenter Server con errores.

Restaurar la instancia de Platform Services Controller con errores

Es posible instalar e implementar Platform Services Controller, así como registrar varias instancias de vCenter Server con la misma instancia de Platform Services Controller. Es posible utilizar vSphere Data Protection para restaurar el entorno si la instancia de Platform Services Controller externa genera errores.

Importante Es posible hacer copias de seguridad únicamente de máquinas virtuales que contienen instancias de vCenter Server, vCenter Server Appliance y Platform Services Controller, y restaurarlas. No puede hacer copias de seguridad y restaurar máquinas físicas que ejecutan vCenter Server a través de vSphere Data Protection.

Requisitos previos

Realice una copia de seguridad de la máquina virtual en la que reside la instancia de Platform Services Controller.

Procedimiento

1 Restaurar una máquina virtual de Platform Services Controller con errores mediante la operación de restauración de emergencia directa a host

  La restauración de emergencia directa a host permite restaurar la máquina virtual que contiene Platform Services Controller cuando vCenter Server deja de estar disponible o cuando el usuario no puede acceder a la interfaz de usuario de vSphere Data Protection mediante vSphere Web Client.

2 Ejecutar el script `vcenter-restore`

Después de completar el proceso de restauración de Platform Services Controller, debe ejecutar el script `vcenter-restore` en las instancias de vCenter Server registradas con el elemento Platform Services Controller restaurado.

Restaurar una máquina virtual de Platform Services Controller con errores mediante la operación de restauración de emergencia directa a host

La restauración de emergencia directa a host permite restaurar la máquina virtual que contiene Platform Services Controller cuando vCenter Server deja de estar disponible o cuando el usuario no puede acceder a la interfaz de usuario de vSphere Data Protection mediante vSphere Web Client.

vSphere Data Protection depende de vCenter Server para muchas de las operaciones esenciales de vSphere Data Protection. Cuando vCenter Server deja de estar disponible, una operación de restauración de emergencia puede restaurar una máquina virtual que contiene la instancia de vCenter Server, vCenter Server Appliance o Platform Services Controller directamente en el host ESXi que se ejecuta en vSphere Data Protection Appliance. La pestaña **Restauración de emergencia** muestra una lista de máquinas virtuales que cuentan con copias de seguridad realizadas por vSphere Data Protection Appliance. Estas máquinas virtuales que contienen instancias de vCenter Server o Platform Services Controller pueden restaurarse como nuevas máquinas virtuales en el host ESXi donde se está ejecutando vSphere Data Protection Appliance. Para conocer las prácticas recomendadas, las recomendaciones y las limitaciones de la operación de restauración de emergencia, consulte la documentación de *vSphere Data Protection*.

Nota En este procedimiento, se utiliza vSphere Data Protection 6.1.3 para describir los pasos. Si utiliza una versión diferente de vSphere Data Protection, los pasos pueden variar.

Procedimiento

1 En un explorador web, desplácese hasta http://*host-name*/ui o http://*host-IP-address*/ui.

   En este caso, *host-name* es el nombre del host ESXi y *host-IP-address* es la dirección IP del host ESXi donde reside vSphere Data Protection Appliance. Inicie sesión como administrador en VMware Host Client.

   a Haga clic con el botón derecho en **Host** desde el inventario de VMware Host Client y seleccione **Desconectar de vCenter Server** en el menú.

   b Haga clic en **Desconectar de vCenter Server** cuando se le pida desasociar el host de vCenter Server.

   Nota Si el host ESXi es de la versión 5.1, inicie sesión en vSphere Client en lugar de hacerlo en VMware Host Client y, en la pestaña **Resumen**, haga clic en **Desasociar host de vCenter Server**.

2 En un explorador web, desplácese hasta la utilidad de configuración de vSphere Data Protection.

   https://*ip_address_VDP_Appliance*:8543/vdp-configure/.

3 En la pestaña **Restauración de emergencia**, seleccione la máquina virtual que servirá de punto de restauración y haga clic en **Restaurar**.

4 En el cuadro de diálogo Credenciales de host, ingrese credenciales de host válidas y haga clic en **Aceptar**.

5 En el cuadro de diálogo Restaurar una copia de seguridad, especifique un nombre nuevo.

6 Seleccione un almacén de datos como destino para la copia de seguridad y haga clic en **Restaurar**.

   Precaución Se enumera el tamaño de capacidad del almacén de datos. Asegúrese de seleccionar un almacén de datos con suficiente espacio en disco para admitir la restauración. Si no hay espacio suficiente, fallará la restauración.

   La máquina virtual restaurada se mostrará en el inventario en el nivel de host de vSphere. No se admite la restauración en una ruta de acceso de inventario más específica.

Ejecutar el script `vcenter-restore`

Después de completar el proceso de restauración de Platform Services Controller, debe ejecutar el script `vcenter-restore` en las instancias de vCenter Server registradas con el elemento Platform Services Controller restaurado.

Procedimiento

1 Inicie sesión en la máquina virtual de vCenter Server.

   - Para vCenter Server Appliance, inicie sesión en el shell del dispositivo como usuario raíz.
   - Para una instancia de vCenter Server instalada en Windows, inicie sesión en el sistema operativo de la máquina virtual como administrador.

2 Compruebe que no haya ningún servicio de vCenter Server en ejecución.

   - Para la instancia de vCenter Server Appliance, ejecute el comando `service-control --status --all` en el shell del dispositivo.
   - Para una instancia de vCenter Server instalada en Windows, en el menú **Inicio** de Windows, seleccione **Panel de control > Herramientas administrativas > Servicios**.

3 Ejecute el script `vcenter-restore` para completar la operación de restauración e iniciar todos los servicios de vCenter Server.

Opción	Acción
Para una instancia de vCenter Server Appliance	Ejecute el script `vcenter-restore` en el shell del dispositivo. `vcenter-restore -u psc_administrator_username -p psc_administrator_password`
Para una instancia de vCenter Server instalada en Windows	1 En el símbolo del sistema de Windows, desplácese hasta el script `vcenter-restore`. De forma predeterminada, el script está ubicado en `C:\Archivos de programa\VMware\vCenter Server\`. 2 Ejecute el script `vcenter-restore`. `vcenter-restore -u psc_administrator_username -p psc_administrator_password` **Nota** Si no se proporcionan argumentos tres veces consecutivas, el script se cierra después de notificar que no se especificaron los argumentos necesarios.

Aquí, *psc_administrator_username* es el nombre de usuario del administrador de vCenter Single Sign-On, que debe estar en formato UPN.

4 Compruebe que todos los servicios de vCenter Server estén en ejecución.

- Para la instancia de vCenter Server Appliance implementada como dispositivo, ejecute el comando `service-control --status --all` en el shell del dispositivo.
- Para la instancia de vCenter Server instalada en Windows, en el menú **Inicio** de Windows, seleccione **Panel de control** > **Herramientas administrativas** > **Servicios**.

Restaurar instancias de vCenter Server con errores

Es posible instalar e implementar Platform Services Controller, así como registrar varias instancias de vCenter Server con la misma instancia de Platform Services Controller. Puede utilizar vSphere Data Protection para restaurar todo el entorno, de modo que si alguna de las instancias de vCenter Server presenta errores, sea posible restaurar la instancia de vCenter Server con errores.

Importante Es posible hacer copias de seguridad únicamente de máquinas virtuales que contienen instancias de vCenter Server, vCenter Server Appliance y Platform Services Controller, y restaurarlas. No puede hacer copias de seguridad y restaurar máquinas físicas que ejecutan vCenter Server a través de vSphere Data Protection.

Debe restaurar cada instancia de vCenter Server con errores.

Requisitos previos

Realice una copia de seguridad de las máquinas virtuales en las que residen las instancias de vCenter Server.

- Restaurar la máquina virtual de vCenter Server con errores a la ubicación original

  Puede restaurar manualmente a la ubicación original la copia de seguridad completa de la imagen de una máquina virtual que contiene una instancia de vCenter Server con el asistente **Restaurar copia de seguridad**.

- Restaurar la máquina virtual de vCenter Server con errores en una nueva ubicación

  Puede restaurar manualmente la copia de seguridad de la imagen completa de una máquina virtual que contenga una instancia de vCenter Server a través del asistente de **restauración de copia de seguridad**.

- Restaurar una máquina virtual de vCenter Server con errores mediante la operación de restauración de emergencia directa a host

  La restauración de emergencia directa a host permite restaurar la máquina virtual que contiene vCenter Server cuando vCenter Server deja de estar disponible o cuando el usuario no puede acceder a la interfaz de usuario de vSphere Data Protection mediante vSphere Web Client.

Pasos siguientes

Encienda la máquina virtual restaurada donde se encuentra la instancia de vCenter Server restaurada.

Restaurar la máquina virtual de vCenter Server con errores a la ubicación original

Puede restaurar manualmente a la ubicación original la copia de seguridad completa de la imagen de una máquina virtual que contiene una instancia de vCenter Server con el asistente **Restaurar copia de seguridad**.

Nota En este procedimiento, se utiliza vSphere Data Protection 6.1.3 para describir los pasos. Si utiliza una versión diferente de vSphere Data Protection, los pasos pueden variar.

Requisitos previos

- Implemente y configure vSphere Data Protection Appliance.
- Haga una copia de seguridad de una máquina virtual con vCenter Server en ejecución. Consulte Usar vSphere Data Protection para hacer copias de seguridad de un entorno de vCenter Server.
- Utilice vSphere Web Client para iniciar sesión en la instancia de vCenter Server que administra el entorno. Inicie sesión como el usuario con privilegios de administrador que se utilizó durante la configuración de vSphere Data Protection.
- Compruebe que la máquina virtual que desea restaurar esté apagada.

Procedimiento

1 En la página de inicio de vSphere Web Client, haga clic en **vSphere Data Protection**.

2 Haga clic en la pestaña **Restaurar**.

3 (opcional) Filtre las copias de seguridad para acotar la búsqueda.

4 Seleccione una máquina virtual de las que se enumeran en la columna Nombre y, a continuación, elija uno o más elementos de copia de seguridad que desee restaurar.

   Al seleccionar una máquina virtual, puede ver la lista de las copias de seguridad realizadas para esa máquina.

5 Haga clic en **Restaurar** para iniciar el asistente **Restaurar copia de seguridad**.

6 En la página Seleccionar copia de seguridad, compruebe que la lista de copias de seguridad sea correcta, quite las copias de seguridad que desee excluir de la operación de restauración y haga clic en **Siguiente**.

7 En la página Establecer opciones de restauración, deje seleccionada la casilla **Restaurar a la ubicación original**.

   Importante Si el disco virtual de la máquina virtual original se extrajo o se eliminó, no podrá restaurar la máquina virtual a su ubicación original. El disco de la máquina virtual (VMDK) deberá restaurarse a una ubicación nueva.

8 (opcional) En **Opciones avanzadas**, seleccione un almacén de datos nuevo para encender la máquina virtual después de que se restaure y volver a conectar la NIC.

9 Haga clic en **Siguiente**.

10 En la página Listo para completar, examine el resumen de sus solicitudes de restauración y haga clic en **Finalizar** para iniciar la operación de restauración.

   Nota Si decide volver a conectar la NIC durante el proceso de restauración, compruebe que la configuración de red de la máquina virtual recién creada sea correcta. Es posible que la NIC de la máquina virtual nueva utilice la misma dirección IP que la máquina virtual original y que eso genere conflictos.

11 Compruebe que no haya ningún servicio de vCenter Server en ejecución.

   - Para la instancia de vCenter Server Appliance, ejecute el comando `service-control --status --all` en el shell del dispositivo.
   - Para una instancia de vCenter Server instalada en Windows, en el menú **Inicio** de Windows, seleccione **Panel de control > Herramientas administrativas > Servicios**.

12 Ejecute el script `vcenter-restore` para completar la operación de restauración e iniciar todos los servicios de vCenter Server.

Opción	Acción
Para una instancia de vCenter Server Appliance	Ejecute el script `vcenter-restore` en el shell del dispositivo. `vcenter-restore -u psc_administrator_username -p psc_administrator_password`
Para una instancia de vCenter Server instalada en Windows	1 En el símbolo del sistema de Windows, desplácese hasta el script `vcenter-restore`. De forma predeterminada, el script está ubicado en `C:\Archivos de programa\VMware\vCenter Server\`. 2 Ejecute el script `vcenter-restore`. `vcenter-restore -u psc_administrator_username -p psc_administrator_password` **Nota** Si no se proporcionan argumentos tres veces consecutivas, el script se cierra después de notificar que no se especificaron los argumentos necesarios.

Aquí, *psc_administrator_username* es el nombre de usuario del administrador de vCenter Single Sign-On, que debe estar en formato UPN.

13 Compruebe que todos los servicios de vCenter Server estén en ejecución.

- Para la instancia de vCenter Server Appliance implementada como dispositivo, ejecute el comando `service-control --status --all` en el shell del dispositivo.
- Para la instancia de vCenter Server instalada en Windows, en el menú **Inicio** de Windows, seleccione **Panel de control** > **Herramientas administrativas** > **Servicios**.

Resultados

Un cuadro de diálogo de información confirma que la operación de restauración se inició correctamente. Puede supervisar el progreso de la restauración en el panel Tareas recientes.

Restaurar la máquina virtual de vCenter Server con errores en una nueva ubicación

Puede restaurar manualmente la copia de seguridad de la imagen completa de una máquina virtual que contenga una instancia de vCenter Server a través del asistente de **restauración de copia de seguridad**.

Nota En este procedimiento, se utiliza vSphere Data Protection 6.1.3 para describir los pasos. Si utiliza una versión diferente de vSphere Data Protection, los pasos pueden variar.

Requisitos previos

- Implemente y configure vSphere Data Protection Appliance.
- Haga una copia de seguridad de una máquina virtual con vCenter Server en ejecución. Consulte Usar vSphere Data Protection para hacer copias de seguridad de un entorno de vCenter Server.

- Utilice vSphere Web Client para iniciar sesión en la instancia de vCenter Server que administra el entorno. Inicie sesión como el usuario con privilegios de administrador que se utilizó durante la configuración de vSphere Data Protection.
- Compruebe que la máquina virtual que desea restaurar esté apagada.

Procedimiento

1 En la página de inicio de vSphere Web Client, haga clic en **vSphere Data Protection**.

2 Haga clic en la pestaña **Restaurar**.

3 (opcional) Filtre las copias de seguridad para acotar la búsqueda.

4 Seleccione una máquina virtual de las que se enumeran en la columna Nombre y, a continuación, elija uno o más elementos de copia de seguridad que desee restaurar.

  Al seleccionar una máquina virtual, puede ver la lista de las copias de seguridad realizadas para esa máquina.

5 Haga clic en **Restaurar** para iniciar el asistente **Restaurar copia de seguridad**.

6 En la página Seleccionar copia de seguridad, compruebe que la lista de copias de seguridad sea correcta, quite las copias de seguridad que desee excluir de la operación de restauración y haga clic en **Siguiente**.

7 En la página Establecer opciones de restauración, deseleccione la casilla **Restaurar a la ubicación original** para establecer las opciones de restauración de cada copia de seguridad que esté restaurando a una ubicación nueva.

8 Escriba el nombre de la máquina virtual nueva y haga clic en **Seleccionar** para elegir un nuevo host para la máquina virtual.

9 Seleccione el almacén de datos en el que desea restaurar la máquina virtual y haga clic en **Siguiente**.

10 (opcional) En **Opciones avanzadas**, seleccione un almacén de datos nuevo para encender la máquina virtual después de que se restaure y volver a conectar la NIC.

11 Haga clic en **Siguiente**.

12 En la página Listo para completar, examine el resumen de sus solicitudes de restauración y haga clic en **Finalizar** para iniciar la operación de restauración.

  Nota Si decide volver a conectar la NIC durante el proceso de restauración, compruebe que la configuración de red de la máquina virtual recién creada sea correcta. Es posible que la NIC de la máquina virtual nueva utilice la misma dirección IP que la máquina virtual original y que eso genere conflictos.

13 Compruebe que no haya ningún servicio de vCenter Server en ejecución.

  - Para la instancia de vCenter Server Appliance, ejecute el comando `service-control --status --all` en el shell del dispositivo.

- Para una instancia de vCenter Server instalada en Windows, en el menú **Inicio** de Windows, seleccione **Panel de control > Herramientas administrativas > Servicios**.

14 Ejecute el script `vcenter-restore` para completar la operación de restauración e iniciar todos los servicios de vCenter Server.

Opción	Acción
Para una instancia de vCenter Server Appliance	Ejecute el script `vcenter-restore` en el shell del dispositivo. `vcenter-restore -u psc_administrator_username -p psc_administrator_password`
Para una instancia de vCenter Server instalada en Windows	1 En el símbolo del sistema de Windows, desplácese hasta el script `vcenter-restore`. De forma predeterminada, el script está ubicado en `C:\Archivos de programa\VMware\vCenter Server\`. 2 Ejecute el script `vcenter-restore`. `vcenter-restore -u psc_administrator_username -p psc_administrator_password` **Nota** Si no se proporcionan argumentos tres veces consecutivas, el script se cierra después de notificar que no se especificaron los argumentos necesarios.

Aquí, *psc_ administrator_ username* es el nombre de usuario del administrador de vCenter Single Sign-On, que debe estar en formato UPN.

15 Compruebe que todos los servicios de vCenter Server estén en ejecución.

- Para la instancia de vCenter Server Appliance implementada como dispositivo, ejecute el comando `service-control --status --all` en el shell del dispositivo.
- Para la instancia de vCenter Server instalada en Windows, en el menú **Inicio** de Windows, seleccione **Panel de control > Herramientas administrativas > Servicios**.

Resultados

Un cuadro de diálogo de información confirma que la operación de restauración se inició correctamente. Puede supervisar el progreso de la restauración en el panel Tareas recientes.

Restaurar una máquina virtual de vCenter Server con errores mediante la operación de restauración de emergencia directa a host

La restauración de emergencia directa a host permite restaurar la máquina virtual que contiene vCenter Server cuando vCenter Server deja de estar disponible o cuando el usuario no puede acceder a la interfaz de usuario de vSphere Data Protection mediante vSphere Web Client.

vSphere Data Protection depende de vCenter Server para muchas de las operaciones esenciales de vSphere Data Protection. Cuando vCenter Server deja de estar disponible, una operación de restauración de emergencia puede restaurar una máquina virtual que contiene la instancia de vCenter Server, vCenter Server Appliance o Platform Services Controller directamente en el host ESXi que se ejecuta en vSphere Data Protection Appliance. La pestaña **Restauración de emergencia** muestra una lista de máquinas virtuales que cuentan con copias de seguridad realizadas por vSphere Data Protection Appliance. Estas máquinas virtuales que contienen

instancias de vCenter Server o Platform Services Controller pueden restaurarse como nuevas máquinas virtuales en el host ESXi donde se está ejecutando vSphere Data Protection Appliance. Para conocer las prácticas recomendadas, las recomendaciones y las limitaciones de la operación de restauración de emergencia, consulte la documentación de *vSphere Data Protection*.

Nota En este procedimiento, se utiliza vSphere Data Protection 6.1.3 para describir los pasos. Si utiliza una versión diferente de vSphere Data Protection, los pasos pueden variar.

Requisitos previos

Realice una copia de seguridad de la máquina virtual de vCenter Server o de vCenter Server Appliance mediante vSphere Data Protection.

Procedimiento

1 En un explorador web, desplácese hasta http://*host-name*/ui o http://*host-IP-address*/ui.

   En este caso, *host-name* es el nombre del host ESXi y *host-IP-address* es la dirección IP del host ESXi donde reside vSphere Data Protection Appliance. Inicie sesión como administrador en VMware Host Client.

   a Haga clic con el botón derecho en **Host** desde el inventario de VMware Host Client y seleccione **Desconectar de vCenter Server** en el menú.

   b Haga clic en **Desconectar de vCenter Server** cuando se le pida desasociar el host de vCenter Server.

   Nota Si el host ESXi es de la versión 5.1, inicie sesión en vSphere Client en lugar de hacerlo en VMware Host Client y, en la pestaña **Resumen**, haga clic en **Desasociar host de vCenter Server**.

2 En un explorador web, desplácese hasta la utilidad de configuración de vSphere Data Protection.

   https://*ip_address_VDP_Appliance*:8543/vdp-configure/.

3 En la pestaña **Restauración de emergencia**, seleccione la máquina virtual que servirá de punto de restauración y haga clic en **Restaurar**.

4 En el cuadro de diálogo Credenciales de host, ingrese credenciales de host válidas y haga clic en **Aceptar**.

5 En el cuadro de diálogo Restaurar una copia de seguridad, especifique un nombre nuevo.

6 Seleccione un almacén de datos como destino para la copia de seguridad y haga clic en **Restaurar**.

   Precaución Se enumera el tamaño de capacidad del almacén de datos. Asegúrese de seleccionar un almacén de datos con suficiente espacio en disco para admitir la restauración. Si no hay espacio suficiente, fallará la restauración.

La máquina virtual restaurada se mostrará en el inventario en el nivel de host de vSphere. No se admite la restauración en una ruta de acceso de inventario más específica.

7 Compruebe que no haya ningún servicio de vCenter Server en ejecución.

- Para la instancia de vCenter Server Appliance, ejecute el comando `service-control --status --all` en el shell del dispositivo.
- Para una instancia de vCenter Server instalada en Windows, en el menú **Inicio** de Windows, seleccione **Panel de control > Herramientas administrativas > Servicios**.

8 Ejecute el script `vcenter-restore` para completar la operación de restauración e iniciar todos los servicios de vCenter Server.

Opción	Acción
Para una instancia de vCenter Server Appliance	Ejecute el script `vcenter-restore` en el shell del dispositivo. `vcenter-restore -u psc_administrator_username -p psc_administrator_password`
Para una instancia de vCenter Server instalada en Windows	1 En el símbolo del sistema de Windows, desplácese hasta el script `vcenter-restore`. De forma predeterminada, el script está ubicado en `C:\Archivos de programa\VMware\vCenter Server\`. 2 Ejecute el script `vcenter-restore`. `vcenter-restore -u psc_administrator_username -p psc_administrator_password` **Nota** Si no se proporcionan argumentos tres veces consecutivas, el script se cierra después de notificar que no se especificaron los argumentos necesarios.

Aquí, *psc_administrator_username* es el nombre de usuario del administrador de vCenter Single Sign-On, que debe estar en formato UPN.

9 Compruebe que todos los servicios de vCenter Server estén en ejecución.

- Para la instancia de vCenter Server Appliance implementada como dispositivo, ejecute el comando `service-control --status --all` en el shell del dispositivo.
- Para la instancia de vCenter Server instalada en Windows, en el menú **Inicio** de Windows, seleccione **Panel de control > Herramientas administrativas > Servicios**.

Restaurar un entorno de vCenter Server con varias instancias de Platform Services Controller

Puede utilizar vSphere Data Protection para restaurar un entorno en el que las instancias de vCenter Server están registradas con diferentes instancias de Platform Services Controller y los datos de infraestructura se replican entre las instancias de Platform Services Controller.

Importante Es posible hacer copias de seguridad únicamente de máquinas virtuales que contienen instancias de vCenter Server, vCenter Server Appliance y Platform Services Controller, y restaurarlas. No puede hacer copias de seguridad y restaurar máquinas físicas que ejecutan vCenter Server a través de vSphere Data Protection.

- Restaurar una única instancia de Platform Services Controller con errores

  El entorno puede contener varias instancias de vCenter Server registradas con diferentes instancias de Platform Services Controller externas que replican sus datos. Puede utilizar vSphere Data Protection para hacer copias de seguridad de todo el entorno y restaurarlo, de modo que si una instancia de Platform Services Controller genera errores, sea posible restaurar la instancia de Platform Services Controller con errores.

- Restaurar todas las instancias de Platform Services Controller con errores

  El entorno puede contener varias instancias de vCenter Server registradas con diferentes instancias de Platform Services Controller externas que replican sus datos. Puede utilizar vSphere Data Protection para hacer copias de seguridad de todo el entorno y restaurarlo. Si todas las instancias de Platform Services Controller generan errores, puede restaurar el entorno.

- Restaurar una instancia de vCenter Server con errores

  Es posible que el entorno contenga varias instancias de vCenter Server registradas con distintas instancias externas de Platform Services Controller y que los datos de infraestructura se repliquen entre las instancias de Platform Services Controller. Puede usar vSphere Data Protection para restaurar cualquier instancia de vCenter Server con errores.

Restaurar una única instancia de Platform Services Controller con errores

El entorno puede contener varias instancias de vCenter Server registradas con diferentes instancias de Platform Services Controller externas que replican sus datos. Puede utilizar vSphere Data Protection para hacer copias de seguridad de todo el entorno y restaurarlo, de modo que si

una instancia de Platform Services Controller genera errores, sea posible restaurar la instancia de Platform Services Controller con errores.

Importante Es posible hacer copias de seguridad únicamente de máquinas virtuales que contienen instancias de vCenter Server, vCenter Server Appliance y Platform Services Controller, y restaurarlas. No puede hacer copias de seguridad y restaurar máquinas físicas que ejecutan vCenter Server a través de vSphere Data Protection.

Procedimiento

1 Redirigir vCenter Server a otra instancia de Platform Services Controller externa

   La unión de las instancias de Platform Services Controller externas en el mismo dominio de vCenter Single Sign-On garantiza la alta disponibilidad del sistema.

2 Implementar una nueva instancia de Platform Services Controller

   Si una instancia de Platform Services Controller tiene errores en un entorno que contiene varias instancias de Platform Services Controller, debe implementar una nueva instancia de Platform Services Controller y unirla a un nodo activo en el mismo dominio y sitio de vCenter Single Sign-On.

3 Redirigir las instancias de vCenter Server a la instancia restaurada de Platform Services Controller

   Después de restaurar una instancia de Platform Services Controller con errores en un entorno que contiene varias instancias de vCenter Server registradas con distintas instancias externas de Platform Services Controller, se deben redirigir las instancias de vCenter Server a la instancia restaurada de Platform Services Controller.

Redirigir vCenter Server a otra instancia de Platform Services Controller externa

La unión de las instancias de Platform Services Controller externas en el mismo dominio de vCenter Single Sign-On garantiza la alta disponibilidad del sistema.

Si una instancia externa de Platform Services Controller deja de responder o si se desea distribuir la carga de una instancia externa de Platform Services Controller, es posible volver a apuntar las instancias de vCenter Server a otra instancia de Platform Services Controller dentro del mismo dominio y sitio.

- Puede redirigir la instancia de vCenter Server a una instancia de Platform Services Controller funcional existente que tenga la capacidad de carga libre en el mismo dominio y el mismo sitio.
- Puede instalar o implementar una nueva instancia de Platform Services Controller en el mismo dominio y el mismo sitio a los que redirigirá la instancia vCenter Server.

Requisitos previos

- Si la instancia de Platform Services Controller antigua no responde, quite el nodo y limpie los datos obsoletos de vmdir mediante la ejecución del comando `cmsso-util unregister`. Para obtener información sobre la retirada de una instancia de Platform Services Controller, consulte https://kb.vmware.com/kb/2106736.
- Compruebe que la instancia antigua y la nueva de Platform Services Controller estén en el mismo dominio y sitio de vCenter Single Sign-On mediante la ejecución del comando `vdcrepadmin -f showservers`. Para obtener información sobre el uso del comando, consulte https://kb.vmware.com/kb/2127057.
- Si desea redirigir una instancia de vCenter Server Appliance que se configuró en un clúster de vCenter HA, elimine la configuración de vCenter HA. Para obtener información sobre la forma de eliminar una configuración de vCenter HA, consulte *Disponibilidad de vSphere*.

Procedimiento

1 Inicie sesión en la instancia de vCenter Server.

   - Para una instancia de vCenter Server Appliance, inicie sesión en el shell de vCenter Server Appliance como raíz.
   - Para una instancia de vCenter Server en Windows, inicie sesión como administrador en la máquina virtual o el servidor físico de vCenter Server.

2 Si la instancia de vCenter Server se ejecuta en Windows, abra el símbolo del sistema de este sistema operativo y desplácese hasta `C:\Archivos de programa\VMware\vCenter Server\bin`.

3 Ejecute el comando `cmsso-util repoint`.

```
cmsso-util repoint --repoint-psc psc_fqdn_or_static_ip [--dc-port port_number]
```

   donde los corchetes ([]) encierran las opciones del comando.

   Aquí, *psc_fqdn_or_static_ip* es el nombre de sistema utilizado para identificar la instancia de Platform Services Controller. El nombre de este sistema debe ser un FQDN o una dirección IP estática.

   Nota El valor de FQDN distingue entre mayúsculas y minúsculas.

   Utilice la opción `--dc-port` *`port_number`* si la instancia de Platform Services Controller se ejecuta en un puerto HTTPS personalizado. El valor predeterminado del puerto HTTPS es 443.

4 Inicie sesión en la instancia de vCenter Server mediante vSphere Web Client para comprobar que la instancia de vCenter Server esté en ejecución y pueda administrarse.

Resultados

La instancia de vCenter Server está registrada con la nueva instancia de Platform Services Controller.

Pasos siguientes

Si redirigió una instancia de vCenter Server Appliance que se configuró en un clúster de vCenter HA, puede volver a configurar el clúster de vCenter HA. Para obtener información sobre la forma de configurar vCenter HA, consulte *Disponibilidad de vSphere*.

Implementar una nueva instancia de Platform Services Controller

Si una instancia de Platform Services Controller tiene errores en un entorno que contiene varias instancias de Platform Services Controller, debe implementar una nueva instancia de Platform Services Controller y unirla a un nodo activo en el mismo dominio y sitio de vCenter Single Sign-On.

Puede implementar una nueva instancia de Platform Services Controller con uno de los métodos de implementación.

- Actualizar un dispositivo de Platform Services Controller mediante la GUI
- Implementar una instancia de vCenter Server Appliance o un dispositivo de Platform Services Controller mediante la CLI
- Instalar vCenter Server y Platform Services Controller en Windows

Después de implementar la nueva instancia de Platform Services Controller, puede redireccionar las instancias de vCenter Server nuevamente a ella.

Redirigir las instancias de vCenter Server a la instancia restaurada de Platform Services Controller

Después de restaurar una instancia de Platform Services Controller con errores en un entorno que contiene varias instancias de vCenter Server registradas con distintas instancias externas de Platform Services Controller, se deben redirigir las instancias de vCenter Server a la instancia restaurada de Platform Services Controller.

Requisitos previos

Compruebe que las instancias externas de Platform Services Controller se encuentren dentro de un único sitio y que repliquen los datos de la infraestructura en un mismo dominio.

Procedimiento

1. Inicie sesión en la instancia de vCenter Server.
   - Para una instancia de vCenter Server Appliance, inicie sesión en el shell de vCenter Server Appliance como raíz.
   - Para una instancia de vCenter Server en Windows, inicie sesión como administrador en la máquina virtual o el servidor físico de vCenter Server.
2. Si la instancia de vCenter Server se ejecuta en Windows, abra el símbolo del sistema de este sistema operativo y desplácese hasta `C:\Archivos de programa\VMware\vCenter Server\bin`.

3 Ejecute el script `cmsso-util`.

```
cmsso-util repoint --repoint-psc psc_fqdn_or_static_ip [--dc-port port_number]
```

donde los corchetes ([]) encierran las opciones del comando.

Aquí, *psc_fqdn_or_static_ip* es el nombre de sistema utilizado para identificar la instancia de Platform Services Controller. El nombre de este sistema debe ser un FQDN o una dirección IP estática.

Utilice la opción `--dc-port port_number` si la instancia de Platform Services Controller se ejecuta en un puerto HTTPS personalizado. El valor predeterminado del puerto HTTPS es 443.

4 Inicie sesión en la instancia de vCenter Server mediante vSphere Web Client para comprobar que la instancia de vCenter Server esté en ejecución y pueda administrarse.

Resultados

La instancia de vCenter Server está registrada con la instancia restaurada de Platform Services Controller.

Restaurar todas las instancias de Platform Services Controller con errores

El entorno puede contener varias instancias de vCenter Server registradas con diferentes instancias de Platform Services Controller externas que replican sus datos. Puede utilizar vSphere Data Protection para hacer copias de seguridad de todo el entorno y restaurarlo. Si todas las instancias de Platform Services Controller generan errores, puede restaurar el entorno.

Importante Es posible hacer copias de seguridad únicamente de máquinas virtuales que contienen instancias de vCenter Server, vCenter Server Appliance y Platform Services Controller, y restaurarlas. No puede hacer copias de seguridad y restaurar máquinas físicas que ejecutan vCenter Server a través de vSphere Data Protection.

Restaure la máquina virtual y los servicios de la instancia de Platform Services Controller de la que se ha realizado una copia de seguridad más recientemente mediante la operación de restauración de emergencia directa a host. Una vez completada la restauración, implemente las nuevas instancias de Platform Services Controller y júntelas con la instancia restaurada de Platform Services Controller. Después de la implementación, puede redireccionar las instancias de vCenter Server a las instancias de Platform Services Controller recientemente implementadas.

Procedimiento

1 Restaurar la máquina virtual de Platform Services Controller con la copia de seguridad más reciente mediante la operación de restauración de emergencia directa a host

La restauración de emergencia directa a host permite restaurar la máquina virtual que contiene Platform Services Controller cuando vCenter Server deja de estar disponible o cuando el usuario no puede acceder a la interfaz de usuario de vSphere Data Protection mediante vSphere Web Client.

2 Ejecutar el script `vcenter-restore`

Después de completar el proceso de restauración de Platform Services Controller, debe ejecutar el script `vcenter-restore` en las instancias de vCenter Server registradas con el elemento Platform Services Controller restaurado.

3 Implementar varias instancias de Platform Services Controller

Si más de una instancia de Platform Services Controller genera errores en un entorno que contiene varias instancias de Platform Services Controller, debe implementar nuevas instancias de Platform Services Controller y unirlas a los nodos activos en el mismo dominio y sitio de vCenter Single Sign-On.

4 Redireccionar las conexiones entre las instancias de vCenter Server y Platform Services Controller

Después de restaurar las instancias de Platform Services Controller con errores en un entorno que contiene varias instancias de vCenter Server registradas con distintas instancias externas de Platform Services Controller, se deben redireccionar las instancias de vCenter Server a los nodos restaurados de Platform Services Controller.

Restaurar la máquina virtual de Platform Services Controller con la copia de seguridad más reciente mediante la operación de restauración de emergencia directa a host

La restauración de emergencia directa a host permite restaurar la máquina virtual que contiene Platform Services Controller cuando vCenter Server deja de estar disponible o cuando el usuario no puede acceder a la interfaz de usuario de vSphere Data Protection mediante vSphere Web Client.

vSphere Data Protection depende de vCenter Server para muchas de las operaciones esenciales de vSphere Data Protection. Cuando vCenter Server deja de estar disponible, una operación de restauración de emergencia puede restaurar una máquina virtual que contiene la instancia de vCenter Server, vCenter Server Appliance o Platform Services Controller directamente en el host ESXi que se ejecuta en vSphere Data Protection Appliance. La pestaña **Restauración de emergencia** muestra una lista de máquinas virtuales que cuentan con copias de seguridad realizadas por vSphere Data Protection Appliance. Estas máquinas virtuales que contienen instancias de vCenter Server o Platform Services Controller pueden restaurarse como nuevas máquinas virtuales en el host ESXi donde se está ejecutando vSphere Data Protection Appliance. Para conocer las prácticas recomendadas, las recomendaciones y las limitaciones de la operación de restauración de emergencia, consulte la documentación de *vSphere Data Protection*.

Nota En este procedimiento, se utiliza vSphere Data Protection 6.1.3 para describir los pasos. Si utiliza una versión diferente de vSphere Data Protection, los pasos pueden variar.

Procedimiento

1 En un explorador web, desplácese hasta http://*host-name*/ui o http://*host-IP-address*/ui.

   En este caso, *host-name* es el nombre del host ESXi y *host-IP-address* es la dirección IP del host ESXi donde reside vSphere Data Protection Appliance. Inicie sesión como administrador en VMware Host Client.

   a Haga clic con el botón derecho en **Host** desde el inventario de VMware Host Client y seleccione **Desconectar de vCenter Server** en el menú.

   b Haga clic en **Desconectar de vCenter Server** cuando se le pida desasociar el host de vCenter Server.

   Nota Si el host ESXi es de la versión 5.1, inicie sesión en vSphere Client en lugar de hacerlo en VMware Host Client y, en la pestaña **Resumen**, haga clic en **Desasociar host de vCenter Server**.

   ---

2 En un explorador web, desplácese hasta la utilidad de configuración de vSphere Data Protection.

   https://*ip_address_VDP_Appliance*:8543/vdp-configure/.

3 En la pestaña **Restauración de emergencia**, seleccione la máquina virtual que servirá de punto de restauración y haga clic en **Restaurar**.

4 En el cuadro de diálogo Credenciales de host, ingrese credenciales de host válidas y haga clic en **Aceptar**.

5 En el cuadro de diálogo Restaurar una copia de seguridad, especifique un nombre nuevo.

6 Seleccione un almacén de datos como destino para la copia de seguridad y haga clic en **Restaurar**.

   Precaución Se enumera el tamaño de capacidad del almacén de datos. Asegúrese de seleccionar un almacén de datos con suficiente espacio en disco para admitir la restauración. Si no hay espacio suficiente, fallará la restauración.

   La máquina virtual restaurada se mostrará en el inventario en el nivel de host de vSphere. No se admite la restauración en una ruta de acceso de inventario más específica.

Ejecutar el script `vcenter-restore`

Después de completar el proceso de restauración de Platform Services Controller, debe ejecutar el script `vcenter-restore` en las instancias de vCenter Server registradas con el elemento Platform Services Controller restaurado.

Procedimiento

1 Inicie sesión en la máquina virtual de vCenter Server.

   - Para vCenter Server Appliance, inicie sesión en el shell del dispositivo como usuario raíz.

- Para una instancia de vCenter Server instalada en Windows, inicie sesión en el sistema operativo de la máquina virtual como administrador.

2 Compruebe que no haya ningún servicio de vCenter Server en ejecución.

- Para la instancia de vCenter Server Appliance, ejecute el comando `service-control --status --all` en el shell del dispositivo.
- Para una instancia de vCenter Server instalada en Windows, en el menú **Inicio** de Windows, seleccione **Panel de control > Herramientas administrativas > Servicios**.

3 Ejecute el script `vcenter-restore` para completar la operación de restauración e iniciar todos los servicios de vCenter Server.

Opción	Acción
Para una instancia de vCenter Server Appliance	Ejecute el script `vcenter-restore` en el shell del dispositivo. `vcenter-restore -u psc_administrator_username -p psc_administrator_password`
Para una instancia de vCenter Server instalada en Windows	1 En el símbolo del sistema de Windows, desplácese hasta el script `vcenter-restore`. De forma predeterminada, el script está ubicado en `C:\Archivos de programa\VMware\vCenter Server\`. 2 Ejecute el script `vcenter-restore`. `vcenter-restore -u psc_administrator_username -p psc_administrator_password` **Nota** Si no se proporcionan argumentos tres veces consecutivas, el script se cierra después de notificar que no se especificaron los argumentos necesarios.

Aquí, *psc_administrator_username* es el nombre de usuario del administrador de vCenter Single Sign-On, que debe estar en formato UPN.

4 Compruebe que todos los servicios de vCenter Server estén en ejecución.

- ◆ Para la instancia de vCenter Server Appliance implementada como dispositivo, ejecute el comando `service-control --status --all` en el shell del dispositivo.
- ◆ Para la instancia de vCenter Server instalada en Windows, en el menú **Inicio** de Windows, seleccione **Panel de control > Herramientas administrativas > Servicios**.

Implementar varias instancias de Platform Services Controller

Si más de una instancia de Platform Services Controller genera errores en un entorno que contiene varias instancias de Platform Services Controller, debe implementar nuevas instancias de Platform Services Controller y unirlas a los nodos activos en el mismo dominio y sitio de vCenter Single Sign-On.

Puede implementar las nuevas instancias de Platform Services Controller con uno de los métodos de implementación.

- Actualizar un dispositivo de Platform Services Controller mediante la GUI

- Implementar una instancia de vCenter Server Appliance o un dispositivo de Platform Services Controller mediante la CLI
- Instalar vCenter Server y Platform Services Controller en Windows

Después de implementar las nuevas instancias de Platform Services Controller, puede redireccionar las instancias de vCenter Server nuevamente a ellas.

Redireccionar las conexiones entre las instancias de vCenter Server y Platform Services Controller

Después de restaurar las instancias de Platform Services Controller con errores en un entorno que contiene varias instancias de vCenter Server registradas con distintas instancias externas de Platform Services Controller, se deben redireccionar las instancias de vCenter Server a los nodos restaurados de Platform Services Controller.

Requisitos previos

Compruebe que las instancias externas de Platform Services Controller se encuentren dentro de un único sitio y que repliquen los datos de la infraestructura en un mismo dominio.

Procedimiento

1 Inicie sesión en la instancia de vCenter Server.

   - Para una instancia de vCenter Server Appliance, inicie sesión en el shell de vCenter Server Appliance como raíz.
   - Para una instancia de vCenter Server en Windows, inicie sesión como administrador en la máquina virtual o el servidor físico de vCenter Server.

2 Si la instancia de vCenter Server se ejecuta en Windows, abra el símbolo del sistema de este sistema operativo y desplácese hasta `C:\Archivos de programa\VMware\vCenter Server\bin`.

3 Ejecute el script `cmsso-util`.

```
cmsso-util repoint --repoint-psc psc_fqdn_or_static_ip [--dc-port port_number]
```

   donde los corchetes ([]) encierran las opciones del comando.

   Aquí, *psc_fqdn_or_static_ip* es el nombre de sistema utilizado para identificar la instancia de Platform Services Controller. El nombre de este sistema debe ser un FQDN o una dirección IP estática.

   Utilice la opción `--dc-port` *`port_number`* si la instancia de Platform Services Controller se ejecuta en un puerto HTTPS personalizado. El valor predeterminado del puerto HTTPS es 443.

4 Inicie sesión en la instancia de vCenter Server mediante vSphere Web Client para comprobar que la instancia de vCenter Server esté en ejecución y pueda administrarse.

Resultados

La instancia de vCenter Server está registrada con la instancia restaurada de Platform Services Controller.

Restaurar una instancia de vCenter Server con errores

Es posible que el entorno contenga varias instancias de vCenter Server registradas con distintas instancias externas de Platform Services Controller y que los datos de infraestructura se repliquen entre las instancias de Platform Services Controller. Puede usar vSphere Data Protection para restaurar cualquier instancia de vCenter Server con errores.

Importante Es posible hacer copias de seguridad únicamente de máquinas virtuales que contienen instancias de vCenter Server, vCenter Server Appliance y Platform Services Controller, y restaurarlas. No puede hacer copias de seguridad y restaurar máquinas físicas que ejecutan vCenter Server a través de vSphere Data Protection.

Debe restaurar cada instancia de vCenter Server con errores.

Requisitos previos

Realice una copia de seguridad de las máquinas virtuales en las que residen las instancias de vCenter Server.

- Restaurar la máquina virtual de vCenter Server con errores a la ubicación original

  Puede restaurar manualmente a la ubicación original la copia de seguridad completa de la imagen de una máquina virtual que contiene una instancia de vCenter Server con el asistente **Restaurar copia de seguridad**.

- Restaurar la máquina virtual de vCenter Server con errores en una nueva ubicación

  Puede restaurar manualmente la copia de seguridad de la imagen completa de una máquina virtual que contenga una instancia de vCenter Server a través del asistente de **restauración de copia de seguridad**.

- Restaurar una máquina virtual de vCenter Server con errores mediante la operación de restauración de emergencia directa a host

  La restauración de emergencia directa a host permite restaurar la máquina virtual que contiene vCenter Server cuando vCenter Server deja de estar disponible o cuando el usuario no puede acceder a la interfaz de usuario de vSphere Data Protection mediante vSphere Web Client.

Restaurar la máquina virtual de vCenter Server con errores a la ubicación original

Puede restaurar manualmente a la ubicación original la copia de seguridad completa de la imagen de una máquina virtual que contiene una instancia de vCenter Server con el asistente **Restaurar copia de seguridad**.

Nota En este procedimiento, se utiliza vSphere Data Protection 6.1.3 para describir los pasos. Si utiliza una versión diferente de vSphere Data Protection, los pasos pueden variar.

Requisitos previos

- Implemente y configure vSphere Data Protection Appliance.
- Haga una copia de seguridad de una máquina virtual con vCenter Server en ejecución. Consulte Usar vSphere Data Protection para hacer copias de seguridad de un entorno de vCenter Server.
- Utilice vSphere Web Client para iniciar sesión en la instancia de vCenter Server que administra el entorno. Inicie sesión como el usuario con privilegios de administrador que se utilizó durante la configuración de vSphere Data Protection.
- Compruebe que la máquina virtual que desea restaurar esté apagada.

Procedimiento

1 En la página de inicio de vSphere Web Client, haga clic en **vSphere Data Protection**.

2 Haga clic en la pestaña **Restaurar**.

3 (opcional) Filtre las copias de seguridad para acotar la búsqueda.

4 Seleccione una máquina virtual de las que se enumeran en la columna Nombre y, a continuación, elija uno o más elementos de copia de seguridad que desee restaurar.

Al seleccionar una máquina virtual, puede ver la lista de las copias de seguridad realizadas para esa máquina.

5 Haga clic en **Restaurar** para iniciar el asistente **Restaurar copia de seguridad**.

6 En la página Seleccionar copia de seguridad, compruebe que la lista de copias de seguridad sea correcta, quite las copias de seguridad que desee excluir de la operación de restauración y haga clic en **Siguiente**.

7 En la página Establecer opciones de restauración, deje seleccionada la casilla **Restaurar a la ubicación original**.

Importante Si el disco virtual de la máquina virtual original se extrajo o se eliminó, no podrá restaurar la máquina virtual a su ubicación original. El disco de la máquina virtual (VMDK) deberá restaurarse a una ubicación nueva.

8 (opcional) En **Opciones avanzadas**, seleccione un almacén de datos nuevo para encender la máquina virtual después de que se restaure y volver a conectar la NIC.

9 Haga clic en **Siguiente**.

10 En la página Listo para completar, examine el resumen de sus solicitudes de restauración y haga clic en **Finalizar** para iniciar la operación de restauración.

Nota Si decide volver a conectar la NIC durante el proceso de restauración, compruebe que la configuración de red de la máquina virtual recién creada sea correcta. Es posible que la NIC de la máquina virtual nueva utilice la misma dirección IP que la máquina virtual original y que eso genere conflictos.

11 Compruebe que no haya ningún servicio de vCenter Server en ejecución.

- Para la instancia de vCenter Server Appliance, ejecute el comando `service-control --status --all` en el shell del dispositivo.
- Para una instancia de vCenter Server instalada en Windows, en el menú **Inicio** de Windows, seleccione **Panel de control > Herramientas administrativas > Servicios**.

12 Ejecute el script `vcenter-restore` para completar la operación de restauración e iniciar todos los servicios de vCenter Server.

Opción	Acción
Para una instancia de vCenter Server Appliance	Ejecute el script `vcenter-restore` en el shell del dispositivo. `vcenter-restore -u psc_administrator_username -p psc_administrator_password`
Para una instancia de vCenter Server instalada en Windows	1 En el símbolo del sistema de Windows, desplácese hasta el script `vcenter-restore`. De forma predeterminada, el script está ubicado en `C:\Archivos de programa\VMware\vCenter Server\`. 2 Ejecute el script `vcenter-restore`. `vcenter-restore -u psc_administrator_username -p psc_administrator_password` **Nota** Si no se proporcionan argumentos tres veces consecutivas, el script se cierra después de notificar que no se especificaron los argumentos necesarios.

Aquí, *psc_administrator_username* es el nombre de usuario del administrador de vCenter Single Sign-On, que debe estar en formato UPN.

13 Compruebe que todos los servicios de vCenter Server estén en ejecución.

- Para la instancia de vCenter Server Appliance implementada como dispositivo, ejecute el comando `service-control --status --all` en el shell del dispositivo.
- Para la instancia de vCenter Server instalada en Windows, en el menú **Inicio** de Windows, seleccione **Panel de control > Herramientas administrativas > Servicios**.

Resultados

Un cuadro de diálogo de información confirma que la operación de restauración se inició correctamente. Puede supervisar el progreso de la restauración en el panel Tareas recientes.

Restaurar la máquina virtual de vCenter Server con errores en una nueva ubicación

Puede restaurar manualmente la copia de seguridad de la imagen completa de una máquina virtual que contenga una instancia de vCenter Server a través del asistente de **restauración de copia de seguridad**.

Nota En este procedimiento, se utiliza vSphere Data Protection 6.1.3 para describir los pasos. Si utiliza una versión diferente de vSphere Data Protection, los pasos pueden variar.

Requisitos previos

- Implemente y configure vSphere Data Protection Appliance.
- Haga una copia de seguridad de una máquina virtual con vCenter Server en ejecución. Consulte Usar vSphere Data Protection para hacer copias de seguridad de un entorno de vCenter Server.
- Utilice vSphere Web Client para iniciar sesión en la instancia de vCenter Server que administra el entorno. Inicie sesión como el usuario con privilegios de administrador que se utilizó durante la configuración de vSphere Data Protection.
- Compruebe que la máquina virtual que desea restaurar esté apagada.

Procedimiento

1 En la página de inicio de vSphere Web Client, haga clic en **vSphere Data Protection**.

2 Haga clic en la pestaña **Restaurar**.

3 (opcional) Filtre las copias de seguridad para acotar la búsqueda.

4 Seleccione una máquina virtual de las que se enumeran en la columna Nombre y, a continuación, elija uno o más elementos de copia de seguridad que desee restaurar.

   Al seleccionar una máquina virtual, puede ver la lista de las copias de seguridad realizadas para esa máquina.

5 Haga clic en **Restaurar** para iniciar el asistente **Restaurar copia de seguridad**.

6 En la página Seleccionar copia de seguridad, compruebe que la lista de copias de seguridad sea correcta, quite las copias de seguridad que desee excluir de la operación de restauración y haga clic en **Siguiente**.

7 En la página Establecer opciones de restauración, deseleccione la casilla **Restaurar a la ubicación original** para establecer las opciones de restauración de cada copia de seguridad que esté restaurando a una ubicación nueva.

8 Escriba el nombre de la máquina virtual nueva y haga clic en **Seleccionar** para elegir un nuevo host para la máquina virtual.

9 Seleccione el almacén de datos en el que desea restaurar la máquina virtual y haga clic en **Siguiente**.

10 (opcional) En **Opciones avanzadas**, seleccione un almacén de datos nuevo para encender la máquina virtual después de que se restaure y volver a conectar la NIC.

11 Haga clic en **Siguiente**.

12 En la página Listo para completar, examine el resumen de sus solicitudes de restauración y haga clic en **Finalizar** para iniciar la operación de restauración.

Nota Si decide volver a conectar la NIC durante el proceso de restauración, compruebe que la configuración de red de la máquina virtual recién creada sea correcta. Es posible que la NIC de la máquina virtual nueva utilice la misma dirección IP que la máquina virtual original y que eso genere conflictos.

13 Compruebe que no haya ningún servicio de vCenter Server en ejecución.

- Para la instancia de vCenter Server Appliance, ejecute el comando `service-control --status --all` en el shell del dispositivo.
- Para una instancia de vCenter Server instalada en Windows, en el menú **Inicio** de Windows, seleccione **Panel de control > Herramientas administrativas > Servicios**.

14 Ejecute el script `vcenter-restore` para completar la operación de restauración e iniciar todos los servicios de vCenter Server.

Opción	Acción
Para una instancia de vCenter Server Appliance	Ejecute el script `vcenter-restore` en el shell del dispositivo. `vcenter-restore -u psc_administrator_username -p psc_administrator_password`
Para una instancia de vCenter Server instalada en Windows	1 En el símbolo del sistema de Windows, desplácese hasta el script `vcenter-restore`. De forma predeterminada, el script está ubicado en `C:\Archivos de programa\VMware\vCenter Server\`. 2 Ejecute el script `vcenter-restore`. `vcenter-restore -u psc_administrator_username -p psc_administrator_password` **Nota** Si no se proporcionan argumentos tres veces consecutivas, el script se cierra después de notificar que no se especificaron los argumentos necesarios.

Aquí, *psc_administrator_username* es el nombre de usuario del administrador de vCenter Single Sign-On, que debe estar en formato UPN.

15 Compruebe que todos los servicios de vCenter Server estén en ejecución.

- Para la instancia de vCenter Server Appliance implementada como dispositivo, ejecute el comando `service-control --status --all` en el shell del dispositivo.
- Para la instancia de vCenter Server instalada en Windows, en el menú **Inicio** de Windows, seleccione **Panel de control > Herramientas administrativas > Servicios**.

Resultados

Un cuadro de diálogo de información confirma que la operación de restauración se inició correctamente. Puede supervisar el progreso de la restauración en el panel Tareas recientes.

Restaurar una máquina virtual de vCenter Server con errores mediante la operación de restauración de emergencia directa a host

La restauración de emergencia directa a host permite restaurar la máquina virtual que contiene vCenter Server cuando vCenter Server deja de estar disponible o cuando el usuario no puede acceder a la interfaz de usuario de vSphere Data Protection mediante vSphere Web Client.

vSphere Data Protection depende de vCenter Server para muchas de las operaciones esenciales de vSphere Data Protection. Cuando vCenter Server deja de estar disponible, una operación de restauración de emergencia puede restaurar una máquina virtual que contiene la instancia de vCenter Server, vCenter Server Appliance o Platform Services Controller directamente en el host ESXi que se ejecuta en vSphere Data Protection Appliance. La pestaña **Restauración de emergencia** muestra una lista de máquinas virtuales que cuentan con copias de seguridad realizadas por vSphere Data Protection Appliance. Estas máquinas virtuales que contienen instancias de vCenter Server o Platform Services Controller pueden restaurarse como nuevas máquinas virtuales en el host ESXi donde se está ejecutando vSphere Data Protection Appliance. Para conocer las prácticas recomendadas, las recomendaciones y las limitaciones de la operación de restauración de emergencia, consulte la documentación de *vSphere Data Protection*.

Nota En este procedimiento, se utiliza vSphere Data Protection 6.1.3 para describir los pasos. Si utiliza una versión diferente de vSphere Data Protection, los pasos pueden variar.

Requisitos previos

Realice una copia de seguridad de la máquina virtual de vCenter Server o de vCenter Server Appliance mediante vSphere Data Protection.

Procedimiento

1 En un explorador web, desplácese hasta http://*host-name*/ui o http://*host-IP-address*/ui.

   En este caso, *host-name* es el nombre del host ESXi y *host-IP-address* es la dirección IP del host ESXi donde reside vSphere Data Protection Appliance. Inicie sesión como administrador en VMware Host Client.

   a Haga clic con el botón derecho en **Host** desde el inventario de VMware Host Client y seleccione **Desconectar de vCenter Server** en el menú.

   b Haga clic en **Desconectar de vCenter Server** cuando se le pida desasociar el host de vCenter Server.

   Nota Si el host ESXi es de la versión 5.1, inicie sesión en vSphere Client en lugar de hacerlo en VMware Host Client y, en la pestaña **Resumen**, haga clic en **Desasociar host de vCenter Server**.

2 En un explorador web, desplácese hasta la utilidad de configuración de vSphere Data Protection.

   https://*ip_address_VDP_Appliance*:8543/vdp-configure/.

3 En la pestaña **Restauración de emergencia**, seleccione la máquina virtual que servirá de punto de restauración y haga clic en **Restaurar**.

4 En el cuadro de diálogo Credenciales de host, ingrese credenciales de host válidas y haga clic en **Aceptar**.

5 En el cuadro de diálogo Restaurar una copia de seguridad, especifique un nombre nuevo.

6 Seleccione un almacén de datos como destino para la copia de seguridad y haga clic en **Restaurar**.

Precaución Se enumera el tamaño de capacidad del almacén de datos. Asegúrese de seleccionar un almacén de datos con suficiente espacio en disco para admitir la restauración. Si no hay espacio suficiente, fallará la restauración.

La máquina virtual restaurada se mostrará en el inventario en el nivel de host de vSphere. No se admite la restauración en una ruta de acceso de inventario más específica.

7 Compruebe que no haya ningún servicio de vCenter Server en ejecución.

- Para la instancia de vCenter Server Appliance, ejecute el comando `service-control --status --all` en el shell del dispositivo.
- Para una instancia de vCenter Server instalada en Windows, en el menú **Inicio** de Windows, seleccione **Panel de control > Herramientas administrativas > Servicios**.

8 Ejecute el script `vcenter-restore` para completar la operación de restauración e iniciar todos los servicios de vCenter Server.

Opción	Acción
Para una instancia de vCenter Server Appliance	Ejecute el script `vcenter-restore` en el shell del dispositivo. `vcenter-restore -u psc_administrator_username -p psc_administrator_password`
Para una instancia de vCenter Server instalada en Windows	1 En el símbolo del sistema de Windows, desplácese hasta el script `vcenter-restore`. De forma predeterminada, el script está ubicado en `C:\Archivos de programa\VMware\vCenter Server\`. 2 Ejecute el script `vcenter-restore`. `vcenter-restore -u psc_administrator_username -p psc_administrator_password` **Nota** Si no se proporcionan argumentos tres veces consecutivas, el script se cierra después de notificar que no se especificaron los argumentos necesarios.

Aquí, *psc_administrator_username* es el nombre de usuario del administrador de vCenter Single Sign-On, que debe estar en formato UPN.

9 Compruebe que todos los servicios de vCenter Server estén en ejecución.

- Para la instancia de vCenter Server Appliance implementada como dispositivo, ejecute el comando `service-control --status --all` en el shell del dispositivo.
- Para la instancia de vCenter Server instalada en Windows, en el menú **Inicio** de Windows, seleccione **Panel de control > Herramientas administrativas > Servicios**.

Solución de problemas de arranque de ESXi

8

En los temas de solución de problemas de arranque de ESXi, se proporcionan soluciones para los problemas que se pueden enfrentar al arrancar ESXi.

Este capítulo incluye los siguientes temas:

El host se detiene inesperadamente durante el arranque cuando comparte un disco de arranque con otro host

Cuando dos hosts o más, ya sean físicos o virtuales, arrancan desde el mismo LUN o desde el mismo disco físico compartido, no pueden usar la misma partición temporal.

Problema

El host se detiene en el arranque cuando comparte un disco de arranque con otro host.

Causa

Dos hosts ESXi o más pueden compartir el mismo LUN o el mismo disco físico. Cuando hay dos hosts de este tipo que, además, tienen configurada la misma partición temporal, cualquiera de los dos hosts puede experimentar un error en el arranque.

Solución

1 Establezca los hosts para que arranquen de manera secuencial y, a continuación, arránquelos.

   Esta configuración permite iniciar los hosts de manera tal que pueda cambiar la partición temporal para uno de ellos.

2 Desde vSphere Web Client, conéctese a vCenter Server.

3 Seleccione el host en el inventario.

4 Haga clic en la pestaña **Administrar**.

5 Haga clic en **Configuración**.

6 En Sistema, seleccione **Configuración avanzada del sistema**.

7 Seleccione **ScratchConfig**.

   El cuadro de texto **ScratchConfig.CurrentScratchLocation** muestra la ubicación actual de la partición desde cero.

8 En el cuadro de texto **ScratchConfig.ConfiguredScratchLocation**, introduzca una ruta de acceso de directorio que sea exclusiva para este host.

   Por ejemplo, **`/vmfs/volumes/`*`DatastoreUUID`*`/`*`DatastoreFolder`***.

9 Reinicie el host para que se apliquen los cambios.

El host no arranca después de instalar ESXi en modo UEFI

Después de instalar ESXi en un equipo host en modo UEFI, la máquina podría generar un error al arrancar.

Problema

Al instalar o actualizar ESXi, el instalador intenta crear una opción de arranque UEFI denominada `VMware ESXi` y convertirla en la opción de arranque predeterminada. Cuando se reinicia después de instalar ESXi, es posible que se produzca un error en el reinicio. Este problema viene acompañado de un mensaje de error similar a `No hay dispositivo de arranque disponible.`

Causa

- Cuando el instalador crea la opción de arranque UEFI, se produce un problema al escribir en la NVRAM de la placa base del host.
- El firmware del host no reconoce el intento de establecer la opción de arranque UEFI como la opción de arranque inicial, o bien el firmware anula el orden de arranque.
- El disco de arranque tiene una tabla de particiones MBR o MSDOS. Debido a una limitación técnica, la opción de arranque UEFI solo se crea para una tabla de particiones GUID Partition Table (GPT).

Nota El firmware UEFI intenta cargar la imagen de arranque desde la partición del sistema EFI, que está basada en FAT, en el disco. El arranque desde la partición del sistema EFI solo funciona si el disco se establece mediante un GPT. Si el disco de arranque tiene una tabla de particiones MBR o MSDOS, se produce un error en el arranque UEFI. No se puede agregar una entrada de arranque para MBR. Si el disco está totalmente consumido por ESXi, no se puede convertir a GPT y debe arrancar en modo BIOS heredado.

Solución

1 Mientras se muestra el mensaje de error en la pantalla, abra el menú de opciones de arranque. Dependiendo del sistema, el menú de opciones de arranque puede abrirse con un método abreviado de teclado, en el menú del BIOS o en una interfaz de BMC, iLO o iDRAC.

2 Compruebe si existe una opción de arranque `VMware ESXi` e intente arrancar desde ella. Si el arranque se realiza correctamente, cambie el orden de arranque y establezca `VMware ESXi` como la opción de primer arranque.

3 Si el problema no se resuelve, seleccione una opción similar a **Agregar opción de arranque**.

   La redacción y la ubicación de la opción podría variar, según el sistema.

4 Seleccione el archivo `\EFI\BOOT\BOOTx64.EFI` en el disco en el que instaló ESXi.

5 Cambie el orden de arranque de manera que el host arranque desde la opción que haya agregado.

Solucionar problemas de instalación o implementación de vCenter Server

9

Los temas de solución de problemas de instalación o implementación de vCenter Server proporcionan soluciones a problemas que podrían surgir durante la instalación de vCenter Server o la implementación de vCenter Server Appliance.

Este capítulo incluye los siguientes temas:

Recopilar registros para solucionar problemas de una instalación o actualización de vCenter Server

Puede recopilar archivos de registro de instalación o actualización de vCenter Server. Si se produce un error en una instalación o actualización, la comprobación de los archivos de registro puede ayudar a identificar el origen del error.

Puede utilizar el asistente de instalación o el método manual para guardar y recuperar archivos de registro de vCenter Server en el caso de un error en la instalación de Windows.

También puede recopilar archivos de registro de implementación de vCenter Server Appliance.

- Recopilar registros de instalación mediante el asistente de instalación

  Puede usar la página Configuración interrumpida del asistente de instalación para desplazarse hasta el archivo `.zip` generado de los archivos de registro de instalación de vCenter Server para Windows.

- Recuperar registros de instalación de forma manual

  Puede recuperar manualmente los archivos de registro de instalación para examinarlos.

- Recopilar archivos de registro de implementación para vCenter Server Appliance

  Si se produce algún error en la implementación de vCenter Server Appliance, puede recuperar los archivos del registro y analizarlos en busca del motivo del error.

- Exportar un paquete de soporte de vCenter Server para solución de problemas

  Puede exportar el paquete de soporte de la instancia de vCenter Server en vCenter Server Appliance para solucionar problemas mediante la dirección URL que aparece en la pantalla de inicio de la DCUI.

Recopilar registros de instalación mediante el asistente de instalación

Puede usar la página Configuración interrumpida del asistente de instalación para desplazarse hasta el archivo `.zip` generado de los archivos de registro de instalación de vCenter Server para Windows.

Si se produce un error en la instalación, aparece la página Configuración interrumpida con las casillas de recopilación de registros seleccionadas de forma predeterminada.

Procedimiento

1 Deje las casillas activadas y haga clic en **Finalizar**.

  Los archivos de instalación se recopilan en un archivo `.zip` en el escritorio, por ejemplo, `VMware-VCS-logs-`*`time-of-installation-attempt`*`.zip`, donde *time-of-installation-attempt* muestra el año, mes, fecha, hora, minutos y segundos del intento de instalación.

2 Recupere los archivos de registro del archivo `.zip` del escritorio.

Pasos siguientes

Analice los archivos de registro para determinar la causa del error.

Recuperar registros de instalación de forma manual

Puede recuperar manualmente los archivos de registro de instalación para examinarlos.

Procedimiento

1 Desplácese hasta las ubicaciones de los archivos de registro de instalación.

  - El directorio `%PROGRAMDATA%\VMware\vCenterServer\logs`, generalmente `C:\ProgramData\VMware\vCenterServer\logs`
  - El directorio `%TEMP%`, generalmente `C:\Users\`*`username`*`\AppData\Local\Temp`

  Los archivos en el directorio `%TEMP%` incluyen `vc-install.txt`, `vminst.log`, `pkgmgr.log`, `pkgmgr-comp-msi.log` y `vim-vcs-msi.log`.

2 Abra los archivos de registro de la instalación en un editor de texto para su análisis.

Recopilar archivos de registro de implementación para vCenter Server Appliance

Si se produce algún error en la implementación de vCenter Server Appliance, puede recuperar los archivos del registro y analizarlos en busca del motivo del error.

La ruta de acceso completa de los archivos de registro aparece en el asistente de implementación de vCenter Server Appliance.

En caso de error en el primer arranque, puede descargar el paquete de soporte en un equipo host Windows y revisar los archivos de registro para determinar qué script de primera opción de arranque produjo el error. Consulte Exportar un paquete de soporte de vCenter Server para solución de problemas.

Procedimiento

1 En la máquina Windows que usa para implementar vCenter Server Appliance, desplácese hasta la carpeta de los archivos de registro.

   Si inició sesión como administrador, la carpeta predeterminada es `C:\Users\Administrator\AppData\Local\VMware\CIP\vcsaInstaller`.

2 Abra los archivos de registro de la instalación en un editor de texto para su análisis.

Exportar un paquete de soporte de vCenter Server para solución de problemas

Puede exportar el paquete de soporte de la instancia de vCenter Server en vCenter Server Appliance para solucionar problemas mediante la dirección URL que aparece en la pantalla de inicio de la DCUI.

También puede recopilar el paquete de soporte del shell de Bash de vCenter Server Appliance mediante la ejecución del script `vc-support.sh`.

El paquete de soporte se exporta en formato `.tgz`.

Procedimiento

1 Inicie sesión en el equipo host de Windows en el que desea descargar el paquete.

2 Abra un explorador web y escriba la URL del paquete de soporte que se muestra en la DCUI.

   https://*appliance-fully-qualified-domain-name*:443/appliance/support-bundle

3 Escriba el nombre de usuario y la contraseña del usuario raíz.

4 Haga clic en **Entrar**.

   El paquete de soporte se descarga como archivo `.tgz` en su equipo Windows.

5 (opcional) Para determinar cuál fue el script de primer arranque que generó un error, examine el archivo `firstbootStatus.json`.

   Si ejecutó el script `vc-support.sh` en el shell de Bash de vCenter Server Appliance, para examinar el archivo `firstbootStatus.json`, ejecute

   ```
   cat /var/log/firstboot/firstbootStatus.json
   ```

Instalar Platform Services Controller después de un error de instalación anterior

Cuando desee replicar los datos de Platform Services Controller, es posible que no pueda asociar un dominio de vCenter Single Sign-On a una instancia de Platform Services Controller existente.

Problema

Al intentar instalar una instancia de Platform Services Controller, ya sea integrada o externa, y asociar Platform Services Controller a un dominio o sitio de vCenter Single Sign-On, la instalación puede producir un error y este error puede dejar datos incompletos en la federación de Platform Services Controller.

Causa

Los datos de Platform Services Controller no se depuran cuando se produce un error en una instalación de Platform Services Controller. Considere la siguiente situación:

1. Instale Platform Services Controller A.
2. Al intentar instalar Platform Services Controller B y asociarlo al mismo dominio que Platform Services Controller A, se produce un error en la instalación.
3. El segundo intento de instalar Platform Services Controller B y asociarlo al mismo dominio que Platform Services Controller A falla, debido a que Platform Services Controller A contiene datos incompletos.

Solución

1. Inicie sesión como administrador en la máquina en la que desea instalar Platform Services Controller A.
2. En la línea de comandos, diríjase al comando `vdcleavefed`.

   El comando `vdcleavefed` está ubicado en `C:\Archivos de programa\VMware\vCenter Server\vmdird\` en Windows y `/usr/lib/vmware-vmdir/bin/` en Linux.
3. Ejecute el comando `vdcleavefed` para eliminar los datos.

   ```
   vdcleavefed -h Platform-Services-Controller-B-System-Name -u Administrator
   ```
4. Instale Platform Services Controller B.

Microsoft SQL Database configurado en modo de compatibilidad no admitido provoca errores en la instalación o actualización de vCenter Server

Se produce un error en la instalación de vCenter Server con una base de datos de Microsoft SQL cuando la base de datos está configurada en modo de compatibilidad con una versión no compatible.

Problema

Aparece el siguiente mensaje de error: `El usuario de base de datos ingresado no tiene los permisos necesarios para instalar y configurar vCenter Server con la base de datos seleccionada. Corrija los siguientes errores: %s`

Causa

La versión de la base de datos debe ser compatible para vCenter Server. En el caso de SQL, aunque la base de datos sea de una versión compatible, si se configura para que se ejecute en modo de compatibilidad con una versión no compatible, se produce este error. Por ejemplo, si SQL 2008 está configurada para que ejecute el modo de compatibilidad de SQL 2000, se presenta este error.

Solución

- Asegúrese de que la base de datos de vCenter Server sea de una versión compatible y no esté configurada en el modo de compatibilidad con una versión no compatible. Consulte las matrices de interoperabilidad de productos VMware en http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php?.

Retirar ESXi y vCenter Server

10

Los temas de retiro ofrecen información sobre la forma de eliminar ESXi y vCenter Server de equipos host.

Este capítulo incluye los siguientes temas:

Desinstalar un host ESXi

Si no desea que el servidor sea un host ESXi, puede desinstalar el equipo host ESXi.

Procedimiento

1. Quite los almacenes de datos de VMFS en los discos internos para que los discos internos ya no se configuren para almacenar máquinas virtuales.
2. Cambie la configuración de arranque en el BIOS para que el host ya no arranque en ESXi.
3. Instale otro sistema operativo en su lugar.

Desinstalar vCenter Server

Debe tener privilegios de administrador para desinstalar VMware vCenter Server.

Importante Si va a utilizar la base de datos PostgreSQL integrada, la desinstalación de vCenter Server hará que se desinstale la base de datos integrada y se perderán todos los datos.

Requisitos previos

Si va a desinstalar el sistema vCenter Server, elimine los hosts del inventario de hosts y clústeres.

Procedimiento

1. Como usuario administrador en el sistema Windows, haga clic en **Inicio > Panel de control > Programas y características**.
2. Seleccione **VMware vCenter Server** en la lista y haga clic en **Quitar**.
3. Haga clic en **Quitar** para confirmar que desea eliminar el programa.

4. Haga clic en **Finalizar**.
5. Reinicie el sistema.